Journal of Global Ethics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rjge20

Moving beyond settlement: on the need for normative reflection on the global management of movement through data

Natasha Saunders

To cite this article: Natasha Saunders (09 Nov 2023): Moving beyond settlement: on the need for normative reflection on the global management of movement through data, Journal of Global Ethics, DOI: 10.1080/17449626.2023.2271001

To link to this article: https://doi.org/10.1080/17449626.2023.2271001

Published online: 09 Nov 2023.

JOURNAL OF GLOBAL ETHICS
https://doi.org/10.1080/17449626.2023.2271001

Routledge
Taylor & Francis Group

Symposium: The Ethics of Border Controls in a Digital Age

OPEN ACCESS

Moving beyond settlement: on the need for normative reflection on the global management of movement through data

Natasha Saunders

School of International Relations, University of St Andrews, St Andrews, UK

ABSTRACT

Normative theorists of migration are beginning to shift their focus away from an earlier obsession with whether the 'liberal' or 'legitimate' state should have a right to exclude, and toward evaluation of how states engage in immigration control. However, with some notable exceptions – such as work of Rebecca Buxton, David Owen, Serena Parekh, and Alex Sager – this work tends not to focus on the global coordination of such control, and is still largely concerned with issues of membership. In this paper I aim to show the value of shifting normative attention to the fundamentally interdependent nature of state control of migration, and the management of all forms of movement – not just settlement. This global management is greatly facilitated by the rapid digitisation of border controls. As such, I outline three aspects of the way digital border controls work – profiling, biometric identification, and the data sharing practices upon which they rest – and highlight ethical challenges of accountability, consent and the reach of the state, and entrenching global inequalities in access to movement. Ultimately, I hope to show that the globally interconnected nature of migration management is a combination of practices that normative theorists of migration should turn their attention to.

ARTICLE HISTORY
Invited contribution received 15 September 2023

KEYWORDS
Digital borders; migration; ethics; AI

Normative theorists of migration are beginning to shift their focus away from an earlier obsession with whether the 'liberal' or 'legitimate' state should have a right to exclude, and toward evaluation of *how* states engage in immigration control. However, with some notable exceptions (Buxton 2023; Owen 2016; 2020; Parekh 2020; Sager 2016), this work tends not to focus on the *global coordination* of such control, and is still largely concerned with issues of membership. In this paper I aim to show the value of shifting normative attention to the fundamentally interdependent nature of state control of migration, and the management of all forms of movement – not just settlement. This global management is greatly facilitated by the rapid digitisation of border controls. As such, I outline three aspects of the way digital border controls work –

CONTACT Natasha Saunders ✉ negs@st-andrews.ac.uk Arts Faculty Building, The Scores, St Andrews, KY16 9AX, UK

profiling, biometric identification, and the data sharing practices upon which they rest – and highlight ethical challenges of accountability, consent and the reach of the state, and entrenching global inequalities in access to movement. Ultimately, I hope to show that the globally interconnected nature of migration management is a combination of practices that normative theorists of migration should turn their attention to.

I take my cue in this paper from Phil Cole's critique of much normative theorising on migration that:

> when debating the right to exclude, we aren't really discussing the right of one liberal state to control its borders but a block of powerful liberal capitalist states preventing the entry of the poor and the unskilled, while at the same time seeking those it considers economically valuable from the 'outside' and maintaining more or less free movement between themselves. (Wellman and Cole 2011, 222)

Cole's insistence that we recognise how states do not impose individual border controls, but rather enforce their borders together rebuts a common defence by advocates of the right to exclude that assumes, to paraphrase David Miller (2005, 196), there is always somewhere else that most people could go. This argument is much more likely to convince if you simply ignore the radically interdependent nature of border controls, the rapidly globalising system of migration management, and the disproportionate influence that a handful of the wealthiest states in the system exercise over movement broadly understood (not just immigration for the purposes of settlement). The way that states coordinate to control the movement of people on a global scale raises specific ethical issues, and casts existing issues in a new light, and thus there is value in approaching the ethics of migration from the perspective of actually existing *global* practice, rather than the ideal abstraction of 'the liberal state' or focusing exclusively on questions of membership. I hope to demonstrate such value by, first, outlining three core aspects of digital border controls; second, demonstrating that these practices combine to form a rapidly developing digital web through which wealthy states co-opt poorer states into doing their migration-related bidding; and third, explaining some of the ethical issues raised by these practices.

Digital control of global movement

Technology has always been central not only to the ability of the state to exercise its core functions, but also in determining what those core functions are. While states have long possessed the *desire* to exercise complete control over movement and territory, their *ability* to do so is largely a function of the means they have at their disposal. The development of digital technologies is helping the state to exercise a greater degree of control over migration, both 'within' and 'beyond' borders. Doing so, however, requires the cooperation of, and coordination with, other states, and with private companies. To see why and how this is the case, we can turn to the role of 'data'. Data is what the state needs and uses to make migration decisions. How we generate data, how states access it, and what they do with it brings into view a rapidly developing global network of migration management, which is largely the creation of, and for the benefit of, wealthy Western states.

Profiling

We often assume that decisions made about our ability to cross a border or to settle in a different state are based solely on our own actions/biography, particularly where these align with the immigration criteria of the state we are trying to enter. While this intuition is not entirely wrong, migration decisions are not, in fact, based solely on what *we* have or have not *done*. Assumptions 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 or might not do in 'the future' also factor into these decisions. In other words, states make use of profiling (a form of predictive analytics) to decide who can or cannot cross borders, where, when and for what purposes. Profiling itself is not a new technique, but the form it takes is changing. Profiles are developed using data mining and analytics tools, which use algorithms to process massive volumes of data collected about, and from, individuals. Algorithms can process greater quantities of data than a person can, and so, their developers and advocates claim, can be used to identify 'connections' between data, people, events, organisations, etc, that indicate a 'likelihood' or 'risk' of something occurring that may elude a human decision-maker. Profiles of what characteristics someone likely to commit terrorist activity, or overstay their visa, would have are developed from large amounts of data gathered not only when we actively provide it in the process of booking an airline ticket, or applying for a visa, but which can also be 'mined' from commercial databases and social media (Patel et al. 2019). 'Our' data is run against the aggregated data 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).

Profiling is intended to identify *potentially risky* subjects who are not yet known to the authorities, rather than identifying known threats. For example, the EU is developing a system of 'screening rules' using data provided during visa and travel authorisation processes (including biographic and financial data, data on employment and information provided about sponsors and contacts, state-level data on epidemic disease risks, and so on). These screening rules will be used to identify individuals not yet known to authorities but who should be considered 'of interest for irregular migration, security or public health purposes due to the fact that they display particular category traits' (Jones 2020, 20). This system is similar to those already in use in the US, such as the Automated Targeting System, which flags individuals as supposed security risks and prevents their travel (Hall 2017, 488). Purely automated decision making is not currently legal, in the EU at least, but developments indicate a trend toward greater automation and reliance on algorithmic data processing. The newly developed ETIAS (European Travel Information and Authorisation System) establishes a new watchlist, against which all applications for travel authorisations will be checked. The watchlist will not just contain data on individuals suspected of having committed or taken part in terrorist or other serious criminal offences, but will also 'include people who it is believed may commit such offenses in the future' (Jones 2020, 22). Being flagged during these profiling processes could result in denial of changes in immigration status, placement on a No-Fly list, denial of a visa-waiver application, increased interrogation, denial of boarding, and detention.

What these profiling mechanisms demonstrate is that the data that we generate or that we actively provide is not only used to assess our own applications for visas or travel authorisations in the here and now, but also 'to train the algorithms that will decide the class of people to which we belong: who to let through and who to flag as high-risk in the future' (Bradley and De Noronha 2022, 60). 'Our' data thus impacts the travel possibilities of others, and their data impacts our own plans, long into the future.

Biometrics and 'secure ID'

Claiming a responsibility to protect the community from threats, states aim to identify everyone seeking to cross their borders (whether on a short- or long-term basis). A global push for digital identification systems is rooted, partly, in this concern, and these systems tend to be biometric, either replacing or supplementing more traditional paper-based identification systems. Biometrics is 'the technology of measuring, analysing and processing the digital representations of unique biological data and behavioural traits' (Ajana 2010, 238): fingerprints, iris scans, voice and facial pattern analysis, and gait analysis. Biometrics can be used in two ways: for identification/recognition, or for verification/authentication. Identification/recognition seeks to determine who someone is, by comparing their biometric to all biometrics in the relevant database(s) – this is a one-to-many comparison. Verification/authentication seeks to determine whether a person is who they claim to be – a one-to-one comparison. The Eurodac database is an example of an identification/recognition system, and a 'trusted traveller' programme is an example of a verification/authentication system.

Using the body to establish 'truths' is also not new (Aas 2006), and border agents have long compared passport photographs with our physical appearance at their desk. Fingerprints and iris scans are, however, considered unique to each individual and so argued to be a much more secure way of determining one's identity. Digital biometric technologies can process a greater number of people more quickly, thus expediting the border crossing of travellers considered 'desirable', but also more 'accurately' identifying those whose movement should be stopped or who should be subjected to greater scrutiny.[1] Visa applicants must provide biometrics for entry to all Western states at a consulate prior to attempting to travel, with refusal to provide one's biometrics resulting in visa refusal. Powerful states also use biometric requirements to influence the identity systems of other states. The USA, 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 have to go through the (more time consuming and expensive) regular visa application process, even just to visit as a tourist.

Data sharing

To function, algorithmic profiling, biometric identification, and a series of other digital border control practices not examined here, require data that we generate about ourselves, including, potentially, data we generate in non-migration-related contexts. When we go about our daily lives we often are not engaging directly with the state, or consciously/deliberately providing data to the state to use for migration purposes. For example, when a person checks their credit score with a view to applying for a mortgage, they are not doing so to engage with their government, let alone any other government. So how does this data – such as occupation, salary level, history of timely payments, people one may be financially linked to – which is often generated in a non-migration context come to play a role in migration management? The short answer is data sharing.

Data sharing happens on several levels and between multiple actors. In the first place it occurs when we provide data to a company running an App or website that we use through agreeing to Terms and Conditions of use or accepting their 'Privacy Policy'.

The next level occurs between companies, usually through the sale of data to 'data brokers' (companies who buy and sell data for profit). Data can also be shared between such companies/brokers and governments, through contracts granting access to collected data. Governments share data acquired between departments/agencies through shared databases. Finally, data can be shared internationally, through data-sharing agreements. The data that we provide could be shared once or it could be shared multiple times, across multiple levels, and it often is not clear who exactly will gain access to our data, when, and what they will use it for. For example, one must agree to Microsoft's privacy policy to use Skype. This policy allows Microsoft to collect a wide range of data from users (including who your contacts are, who you call, for how long, and so on), but is ambiguous on the extent to which this data will be shared with others, who those others are, and for what purposes shared data will be used. Most people do not read, and would not understand, these policies. We click 'Yes' or 'Agree' because we must if we want to use that app/service/website, but once the company 'owns' that data, they can then sell it to others (Thatcher, O'Sullivan, and Mahmoudi 2016). The US Immigration and Customs Enforcement agency (ICE), for example, has purchased access to the Consolidated Lead Evaluation and Reporting (CLEAR) system from West Publishing Corporation, gaining access to phone records, consumer and credit bureau data, healthcare provider content, utilities data, and data from social networks and chatrooms (Privacy International 2020a, 17). ICE uses this data, often provided by individuals to companies in non-migration-related contexts, to inform its immigration enforcement activities. Indeed, multiple countries harvest data from commercial databases, use them for their own purposes, and then share them with agencies from other countries (Bellanova and de Goede 2020, 107).

Sometimes, though, we do consciously and directly engage with the state, providing certain data in the process – such as when we seek healthcare, or apply for housing support. This data can also be shared widely – between government departments, and even between states for migration-related purposes. For example, the UK Home Office can share data of immigration status applicants, including with other government departments, the police, and foreign governments. It can also request access to data that such individuals may have provided to other agencies/departments, including in foreign countries (Guild 2019, 271). Cooperation agreements between developed and developing states also involve the sharing of data on people. A common condition of EU development aid, particularly through the EU Trust Fund for Africa, is the gathering and sharing of data with the EU, or with individual Member States, about people on the move. FRONTEX, the EU's border security agency, also engages in social media monitoring for what it calls 'preventive risk analysis purposes', and shares information it generates with Member States (Latonero and Kift 2018, 6–7).

A global network of western control

As has been extensively documented in work on critical border studies, states have been progressively building externalised border control systems over the past few decades, and profiling, data sharing and biometric ID systems are central to these efforts. The purpose of border externalisation is to push migration control as far from the physical demarcations of state territory as possible – to interdict, intercept and prevent the *travel* (not just the settlement) of undesirable or risky subjects long before they might physically enter a state's territory: 'the Border Police officer at the port of arrival will become the last line of defence rather than the first … dealing with exceptions rather than checking travellers and granting them admission to the country on the spot' (Hayes 2009, 35). The wealthiest and most powerful states in the international system began this process, initially building cooperation amongst themselves, and have progressively been incorporating more and more states in order to exert greater control over global movement. Data gathering and sharing is integral to the operation of these externalised border controls. To see why, we can take the example of the US No-Fly list. The data used to include someone on the List has to come from somewhere – thus has to be shared with the US – but the No-Fly list can only prevent individuals from reaching US territory if those individuals are prevented from taking circuitous routes, and not just direct ones. Thus, alerts must be triggered whenever/wherever a person on the list tries to travel (regardless of their destination). These systems thus work, or at least are intended to work, to prevent undesirable or 'risky' subjects from using global travel infrastructures, particularly airlines. They are not developed primarily for governing access to membership once 'inside' the state, but to prevent 'undesirables' from accessing state territory in the first place. Despite political rhetoric to the contrary, states know that they cannot control migration on their own. They know they must cooperate and coordinate with other states to do so.

Governments, however, often lack the technical expertise to build algorithmic systems used in profiling, or to build interoperable databases and ensure that data can be shared between them. Similarly, governments often do not have the expertise to build the tools to capture, analyse and share biometric data. It is private companies that do this work, and these companies tend to be Western companies, including military/defence contractors. Governments can often incentivise the development of new border control tech through a promise of contracts, but this process is often driven by the commercial interests of private companies (Lemberg-Pedersen, Hansen, and Halpern 2020). Through development aid, funds to purchase these products are provided to states identified as (potential) 'transit' or origin states for migrants. For example, through the EU Trust Fund for Africa, a key focus of aid has been 'capacity building' through modernisation of state identification and surveillance systems (Bradley and De Noronha 2022, 55). In 2020, Privacy International revealed tens of millions of Euros spent under the EU Trust Fund projects for the development of biometric identity systems (Privacy International 2020b). These EU-funded technologies have been used by recipient governments, including Senegal and Cote d'Ivoire, to exert increasing degrees of control over their own populations, including by denying civil freedoms and squashing political opposition (Bradley and De Noronha 2022, 55). In order to exert greater control of global movement, the EU (and the US) pushes the development of biometric identification systems and of increased law enforcement surveillance capacity in states with poor human rights records and authoritarian governments. These states are thus co-opted into a rapidly developing globalised migration management system crafted by, and for the benefit of, the wealthiest states in the system. Indeed, the provision of development aid, such as through the EU Trust Fund, is often conditional on recipient state cooperation with donor states in their migration management objectives (Raty and Shilhav 2020), and the majority of funds allocated for 'Migration Governance' projects focus on 'returns' and 'containment and control' of would-be travellers (Raty and Shilhav 2020, 13).

The proliferation and sharing of data – not only between government departments, but between private companies and states, and between states – is thus 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). In other words, a global digital web is developing which enables states – particularly Western states – to access increasing amounts of data about would-be travellers/migrants and use this data to feed into efforts to control global movement.

Ethical issues

We do need to be wary of feeding into hype around Artificial Intelligence, and the power of digital border control technologies. Their operation is not seamless; the control they provide over global movement is not total; they have not completely replaced human decision-makers; and they are not beyond (legal) challenge. The global network of migration management is not, yet, a panopticon. However, this kind of total control is clearly the goal toward which states are working, and their current use, even though not seamless, still raises profound ethical issues. I highlight three of the most pressing issues below.

Accountability and contestability

One way of understanding accountability is as the requirement of a decision-maker/authority 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. With algorithmic systems, such as profiling systems – it is not immediately clear who/what we should expect to give an account of itself (Schuppli 2014). Why is this the case? 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 algorithmic systems in a timely fashion is severely limited. Accountability is undermined by limitations in understanding, technical knowledge, and time. The term 'black box' is often used to convey the opaque nature of algorithmic systems. Even if it were possible to crack open the box, of a visa profiling system, for example, and shine a light on its inner workings, we (or even a group of experts) would not necessarily be able to *understand* the behaviour of that system and the rationale behind its outputs. As Faveratto et al. highlight, such systems 'might intrinsically transcend human comprehension since algorithms do not make use of theories or contexts as in regular human-based decision-making' (2019, 17). This is especially the case for algorithmic systems 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 original programmers (Panagia 2021, 116). Temporal limitations mean that even if we could 'see inside' an algorithmic system, what we would see 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 (Ananny and Crawford 2018, 982).

What is so important to recognise about, for example, the use of predictive analytics to profile travellers, is that the connections that the algorithms make to build the profile and then to determine a 'hit' or a 'match' to screening rules, 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 doesn't 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 are assigned to us and used to 'diminish a person's range of future [migration] options' (Ajana 2015, 69). The fundamental issue here is that the ability of individuals to contest decisions that they believe to be wrong/discriminatory/harmful is critically undermined by these intrinsic barriers to accountability. 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 legal redress for such decisions/harms.[2]

Consent and the reach of the state(s)

It is almost impossible today not to generate data about oneself, and 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 is it truly consent if we have no other realistic option? Terms and Conditions could certainly make it much clearer that our data – even if anonymised – can be sold and used for a range of purposes beyond the purpose for which we originally provided it. But if there is no option to opt-out of this data transfer and still use a service/app/website, then the choice we have isn't between providing data about ourselves or not. It is, rather, using a service/app/website or not. This may not matter a great deal if the app/service/website we are trying to use is something relatively trivial, such as a restaurant booking app (although we have no way of knowing whether the use of such an app would remain 'trivial' in, for example, a migration context). But there are other services/apps/websites 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.

This issue of consent is closely related to 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). What is particularly important to recognise in the migration context is that 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. Data moves in a very different way to people, is often repurposed in different contexts, and has a variety of life-cycles. Data that we consent to provide in one context may be erased after a certain period of time, but in that time may have been shared with other actors and take on a new life-cycle and purpose. We really have no way of knowing where in the world our data *could* end up and what it *could* be used for. 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)

Exacerbating existing inequalities in movement and rights

While there is debate in the normative literature over whether state control of membership policy gives rise to justice claims on the part of would-be migrants from poorer states, the control exercised by wealthy states over global movement in general raises the stakes of this debate: the control that wealthy states exercise is not merely over access to citizenship, but is control over the ability of people from poorer states to travel at all – including, in some cases, to even leave their own state.

Citizens of many less developed states face a slightly different challenge relating to the gathering and sharing of data to citizens of wealthy states: paucity of ('reliable') data. The comparative paucity of 'reliable' data produced by/about citizens of poorer states is considered by wealthier states to be a particular issue. This concern partly drives the glaring imbalance in access to visa-waivers for citizens of rich vs poor countries, and visa acceptance rates, but is also driving wealthy, Western, states to push for biometric identification systems, and to fund surveillance and data gathering tools, in poor states.

Individuals from the 'Global South' are, thus, subjected to an excess of bordering based on the assumption that even tourist visas are sought to circumvent immigration rules and gain entry to a state under false pretences. Additionally, however, many of the same countries are comparatively tech and data poor, and the data that their citizens can and do produce is often considered untrustworthy and unreliable, thus making any travel they may engage in potentially 'risky'. A kind of 'global firewall' is thus developing: 'If you are in this domain [the West] you can move pretty easily; but it is really hard to get into it if you are coming from a tribal area or some place where your identity is purely social and it is not stored in any electronic media' (Longo 2018, 217).

The development of such ID systems in authoritarian states and other states with poor human rights records leads to a host of problems. Increased capacity to identify individuals using their bodies, and increased state surveillance capacity, exacerbates marginalisation of already marginalised communities and compounds human rights abuses. For example, a recent report on the conditions experienced by Rohingya minorities in India, Bangladesh and Myanmar, and current efforts to develop and implement digital ID systems in each of these states, highlighted that the already precarious position of the Rohingya could deteriorate even more through the development of biometric ID systems (Brinham et al. 2020). By making individuals more easily identifiable, they are made more vulnerable to abuse and repression. A related issue is of particular importance for those fleeing persecution, such as the Rohingya. 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 one 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. We might think, then, that the efforts to create secure biometric ID systems for all would be a wholly good thing, but this would be too hasty as we cannot ignore the socio-political contexts of the states in which biometric ID systems are being developed.

There are, thus, significant problems that arise from the desire of Western states to push for such identity systems globally, particularly in states with poor human rights records, and with authoritarian governments, where such systems can compound the human rights abuses suffered by minorities and marginalised people.

Conclusion

What I hope to have shown in this paper is that the ways in which states cooperate and coordinate to manage movement of people globally poses a challenging set of ethical issues. Settling the question of whether a state should have a right to exercise control over the conditions of membership will not provide normative guidance to help address the ethical issues highlighted above. States are attempting to collectively manage global movement in general, not only settlement/membership. They are doing this by implementing systems that rely on digital technologies that pose challenges of accountability, contestability, consent, and who/what should have access to our data, how it should be used, and for what purposes. In my own work to come I aim to offer some normative guidance on these questions. I hope that other normative theorists will join in that endeavour.

Notes

1. It is not only states who gather biometric data. Humanitarian organisations such as UNHCR also collect and share biometric data on individuals under their care, raising significant concerns about the safety of those individuals. See, for example Jacobsen (2015; 2017), Jacobsen and Sandvik (2018).
2. For more on how the law is strategically deployed by border-externalising states in order to limit access to rights and redress, see Shachar (2020).

Notes on contributor

Natasha Saunders is a Lecturer in International Relations and International Political Theory at the University of St Andrews, Scotland. Her research sits at the intersection of global politics and political theory, focusing on contemporary social and political thought as a framework for analysing pressing global issues. She has a particular interest in issues of forced migration, human rights, and digital border control practices, and in conceptualisations of, and questions about, political responsibility, social justice, political subjectivity, and agency.

References

Aas, Katja Franko. 2006. "'The Body Does Not Lie': Identity, Risk and Trust in Technoculture." *Crime, Media, Culture: An International Journal* 2 (2): 143–158. https://doi.org/10.1177/1741659006065401.

Adey, Peter. 2009. "Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body." *Environment and Planning D: Society and Space* 27 (2): 274–295. https://doi.org/10.1068/d0208.

Ajana, Btihaj. 2010. "Recombinant Identities: Biometrics and Narrative Bioethics." *Journal of Bioethical Inquiry* 7 (2): 237–258. https://doi.org/10.1007/s11673-010-9228-4.

Ajana, Btihaj. 2015. "Augmented Borders: Big Data and the Ethics of Immigration Control." *Journal of Information, Communication and Ethics in Society* 13 (1): 58–78. https://doi.org/10.1108/JICES-01-2014-0005.

Ananny, Mike, and Kate Crawford. 2018. "Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." *New Media & Society* 20 (3): 973–989. https://doi.org/10.1177/1461444816676645.

Bellanova, Rocco, and Marieke de Goede. 2020. "The Algorithmic Regulation of Security: An Infrastructural Perspective." *Regulation & Governance* 16 (1): 102–118. https://doi.org/10.1111/rego.12338.

Bradley, Gracie Mae, and Luke De Noronha. 2022. *Against Borders: The Case for Abolition*. London: Verso.

Brinham, Natalie, Jessica Field, Anubhav Tiwari, Jaivet Ealom, Jose Arraiza, and Amal de Chickera. 2020. *Locked In and Locked Out: The Impact of Digital Identity Systems on Rohingya Populations*. The Institute on Statelessness and Inclusion. https://files.institutesi.org/Locked_In_Locked_Out_The_Rohingya_Briefing_Paper.pdf.

Broeders, Dennis, and James Hampshire. 2013. "Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe." *Journal of Ethnic and Migration Studies* 39 (8): 1201–1218. https://doi.org/10.1080/1369183X.2013.787512.

Buxton, Rebecca. 2023. "Justice in Waiting: The Harms and Wrongs of Temporary Refugee Protection." *European Journal of Political Theory* 22 (1): 51–72. https://doi.org/10.1177/1474885120973578.

Favaretto, Maddalena, Eva De Clercq, and Bernice Simone Elger. 2019. "Big Data and Discrimination: Perils, Promises and Solutions. A Systematic Review." *Journal of Big Data* 6 (1): 1–27. https://doi.org/10.1186/s40537-019-0177-4.

Guild, Elspeth. 2019. "Data Rights: Claiming Privacy Rights Through International Institutions." In *Data Politics: Worlds, Subjects, Rights*, edited by Didier Bigo, Engin F. Isin, and Evelyn Sharon Ruppert, 267–284. Abingdon: Routledge.

Hall, Alexandra. 2017. "Decisions at the Data Border: Discretion, Discernment and Security." *Security Dialogue* 48 (6): 488–504. https://doi.org/10.1177/0967010617733668.

Hayes, Ben. 2009. *NeoConopticon: The EU 'Security-Industrial Complex'*. Statewatch and the Tansnational Institute. https://www.statewatch.org/media/documents/analyses/neoconopticon-report.pdf.

Jacobsen, Katja Lindskov. 2015. "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees." *Security Dialogue* 46 (2): 144–164. https://doi.org/10.1177/0967010614552545.

Jacobsen, Katja Lindskov. 2017. "On Humanitarian Refugee Biometrics and New Forms of Intervention." *Journal of Intervention and Statebuilding* 11 (4): 529–551. https://doi.org/10.1080/17502977.2017.1347856.

Jacobsen, Katja Lindskov, and Kristin Bergtora Sandvik. 2018. "UNHCR and the Pursuit of International Protection: Accountability Through Technology?" *Third World Quarterly* 39 (8): 1508–1524. https://doi.org/10.1080/01436597.2018.1432346.

Jones, Chris. 2020. "Automated Suspicion: The EU's New Travel Surveillance Initiatives." *Statewatch*. https://www.statewatch.org/media/1235/sw-automated-suspicion-full.pdf.

Latonero, Mark, and Paula Kift. 2018. "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control." *Social Media + Society* 4 (1): 1–11. https://doi.org/10.1177/2056305118764432.

Lemberg-Pedersen, Martin, Johanne Rübner Hansen, and Oliver Joel Halpern. 2020. *The Political Economy of Entry Governance, ADMIGOV Deliverable 1.3*. Aalborg University. http://admigov.eu/upload/Deliverable_D13_Lemberg-Pedersen_The_Political_Economy_of_Entry_Governance.pdf.

Longo, Matthew. 2018. *The Politics of Borders: Sovereignty, Security and the Citizen After 9/11*. Cambridge: Cambridge University Press.

Miller, David. 2005. "Immigration: The Case for Limits." In *Contemporary Debates in Applied Ethics*, edited by Andrew I. Cohen and Christopher Heath Wellman, 193–206. Malden, MA: Black.

Owen, David. 2016. "Refugees, Fairness and Taking up the Slack: On Justice and the International Refugee Regime." *Moral Philosophy and Politics* 3 (2). https://doi.org/10.1515/mopp-2016-0001.

Owen, David. 2020. "Migration, Structural Injustice and Domination on 'Race', Mobility and Transnational Positional Difference." *Journal of Ethnic and Migration Studies* 46 (12): 2585–2601. https://doi.org/10.1080/1369183X.2018.1561067.

Panagia, Davide. 2021. “On the Possibilities of a Political Theory of Algorithms.” *Political Theory* 49 (1): 109–133. https://doi.org/10.1177/0090591720959853.

Parekh, Serena. 2020. *No Refuge: Ethics and the Global Refugee Crisis*. Oxford: Oxford University Press.

Patel, Faiza, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh. 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. 2020a. *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*. London: Privacy International. https://www.privacyinternational.org/sites/default/files/2020-05/2020.3%20PI%20submission%20UN%20WG%20mercenaries.pdf.

Privacy International. 2020b. *Here’s How a Well-Connected Security Company Is Quietly Building Mass Biometric Databases in West Africa with EU Aid Funds*. Privacy International. http://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.

Raty, Tuuli, and Raphael Shilhav. 2020. “The EU Trust Fund for Africa: Trapped Between Aid Policy and Migration Politics.” *Oxfam*. https://doi.org/10.21201/2020.5532.

Sager, Alex. 2016. “Methodological Nationalism, Migration and Political Theory.” *Political Studies* 64 (1): 42–59. https://doi.org/10.1111/1467-9248.12167.

Schuppli, Susan. 2014. “Deadly Algorithms: Can Legal Codes Hold Software Accountable for Code That Kills?” *Radical Philosophy* (187). https://www.radicalphilosophy.com/commentary/deadly-algorithms.

Shachar, Ayelet. 2020. *The Shifting Border: Ayelet Shachar in Dialogue*. Manchester: Manchester University Press.

Thatcher, Jim, David O’Sullivan, and Dillon Mahmoudi. 2016. “Data Colonialism Through Accumulation by Dispossession: New Metaphors for Daily Data.” *Environment and Planning D: Society and Space* 34 (6): 990–1006. https://doi.org/10.1177/0263775816633195.

Wellman, Christopher Heath, and Phillip Cole. 2011. *Debating the Ethics of Immigration: Is There a Right to Exclude? Debating the Ethics of Immigration*. Oxford University Press. https://oxford.universitypressscholarship.com/view/10.1093acprof:osobl/9780199731732.001.0001/acprof-9780199731732.