Hall, Lucy B.; Clapton, William

Article

Programming the machine: Gender, race, sexuality, AI, and the construction of credibility and deceit at the border

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Hall, Lucy B.; Clapton, William (2021) : Programming the machine: Gender, race, sexuality, AI, and the construction of credibility and deceit at the border, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 4, pp. 1-23,
https://doi.org/10.14763/2021.4.1601

This Version is available at:
https://hdl.handle.net/10419/250400

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Programming the machine: gender, race, sexuality, AI, and the construction of credibility and deceit at the border

Lucy Hall *University of Amsterdam*
William Clapton *University of New South Wales*

DOI: https://doi.org/10.14763/2021.4.1601

Published: 7 December 2021
Received: 11 October 2020 **Accepted:** 29 April 2021

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Hall, L. & Clapton, W. (2021). Programming the machine: gender, race, sexuality, AI, and the construction of credibility and deceit at the border. *Internet Policy Review*, *10*(4). https://doi.org/10.14763/2021.4.1601

Keywords: Artificial intelligence, Risk

Abstract: There is increasing recognition of the significance of the political, social, economic, and strategic effects of artificial intelligence (AI). This raises important ethical questions regarding the programming, use, and regulation of AI. This paper argues that both the programming and application of AI are inherently (cis)gendered, sexualised and racialised. AI is, after all, programmed by humans and the issue of who trains AI, teaches it to learn, and the ethics of doing so are therefore critical to avoiding the reproduction of (cis)gendered and racist stereotypes. The paper's empirical focus is the EU-funded project iBorderCtrl, designed to manage security risks and enhance the speed of border crossings for third country nationals via the implementation of several AI-based technologies, including facial recognition and deception detection. By drawing together literature from 1) risk and security 2) AI and ethics/migration/asylum and 3) race, gender, (in)security, and AI, this paper explores the implications of lie detection for both regular border crossings and refugee protection with a conceptual focus on the intersections of gender, sexuality, and race. We argue here that AI border technologies such as iBorderCtrl pose a significant risk of both further marginalising and discriminating against LGBT persons, persons of colour, and asylum seekers and reinforcing existing non entree practices and policies.

This paper is part of **Feminist data protection**, a special issue of *Internet Policy Review* guest-edited by Jens T. Theilen, Andreas Baur, Felix Bieker, Regina Ammicht Quinn, Marit Hansen, and Gloria González Fuster.

Introduction

This article considers the ethics and transformative potential of AI in relation to risk management, border control, and asylum seekers within the context of the EU-funded 'iBorderCtrl', or 'Intelligent Portable Control System' pilot project. Specifically, we are interested in the use of AI technologies at border entry points and their impact on *both* regular crossings at the EU's external borders and asylum seekers within the context of existing *non entree* policies and practices (Gammeltoft-Hansen and Hathaway, 2015). Given a recent EU Commission proposal for a regulation harmonising the rules on AI, including in the areas of migration, asylum, and border control management (2021a, p. 28), we find it timely to reflect on both the potential implications of the increased use of AI technologies at border crossings and possibly in refugee status decision making. In doing so, we provide a novel contribution to the literatures on Critical Security Studies, AI, border control, and refugee protection. The aforementioned EU Commission proposal notes that the 'accuracy, non-discriminatory nature and transparency' of AI systems used in migration, asylum and border control makes them 'particularly important' (EU Commission, 2021a, p. 28). We argue, however, that the use of AI in border management may not be as accurate as assumed, resulting in discrimination against marginalised groups of regular travellers, particularly LGBT persons, and put asylum seekers who have experienced gendered, sexualised, and racialised forms of violence and persecution at risk of being returned to countries where they face inhuman and degrading treatment. The use of AI in border management may reinforce already existing *non-entree* mechanisms that block physical departure by air, sea, and land (Ghezelbash and Tan, 2020, p. 670). *Non entree* measures aim to deter asylum seekers and attempt to circumvent states' *non refoulement responsibilities* (Ghezelbash and Tan, 2020). It is noteworthy, but perhaps not surprising that both *non entree* and *non refoulement* practices have intensified during the COVID-19 pandemic (Ghezelbash and Tan, 2020).

Our argument expands on the literature that has established the ways in which the programming of AI and its application are inherently (cis)gendered, sexualised, and racialised (Wilcox, 2017). AI is, after all, programmed by humans and the issue of who trains AI, teaches it to learn, deploys it, and the ethics of doing so are

therefore critical to avoiding the reproduction of (cis)gendered, and racist stereotypes. Unfortunately, the deployment of iBorderCtrl, and AI border technologies more broadly, have raised issues including racialised and gendered forms of discrimination and marginalisation. European borderlands, and migrants and asylum seekers crossing through them, have become key sites of surveillance and data-gathering for the purposes of risk management. Borders, migrants, and asylum seekers have been subject to intense scrutiny and the application of a range of technologies, including AI, to manage perceived risks across the Western world (Bigo, 2014; Stachowitsch and Sachseder, 2019). While we acknowledge similar efforts to those of the EU discussed below in countries such as Canada and the US, we are drawn to an analysis of the EU's application of AI in border control due to the scale of the EU's investment and the intensity of its interest in AI border technologies.

Frontex, the EU's border and coast guard agency, has a significant interest in AI, publishing a recent report that explores AI technologies in relation to enhancing its capabilities to address border security risks and challenges (Frontex Research and Innovation Unit, 2021a). We follow the European Commission's Independent High Level Expert Group on AI (2019, p. 6) in defining AI as:

> *Systems (including hardware and software) that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information derived from this data and deciding the best action(s) to take to achieve the given goal.*

Data gathering, algorithmic calculation, biometric identification, and data-driven deception and emotion detection have been, or are being, deployed to borders as part of what Amoore (2009) labels 'algorithmic war'. This is but one aspect of the increasingly widespread application of AI and the growing recognition of its political, social, economic, and strategic effects.

AI's ubiquity and its application in security and risk management initiatives raises several issues, including the protection of privacy, the accuracy and efficacy of AI systems, and the assumptions and processes of data collection that inform the programming and functioning of AI. This last issue, the programming of AI, is particularly crucial. Just as scholars working on recent Western approaches to (border) security and risk management have identified the cultural, racial, sexualised, and gendered logics which inform these approaches (Amoore, 2009; Aradau and Van

Munster, 2009; Maguire, 2012; Stachowitsch and Sachseder, 2019) so too are AI technologies gendered, sexualised, and racialised. That is, they can reproduce and reify gendered and racialised assumptions that produce discriminatory outcomes and reinforce discriminatory attitudes towards particular populations that are othered and, on the basis of this othering, presumed to be 'risky' in ways that white populations are not (Noble, 2018; Garcia, 2016; Browne, 2015).

The remainder of this article proceeds as follows. We first explore the salience of risk to understand the ways in which border security is understood and operationalised. We argue here that risk is not a neutral or natural 'thing'; rather it is fundamentally embodied, racialised, and gendered. Risk is a discursive construct based on imaginations of potential futures. Following from this discussion of risk and border management, we then consider some of the issues associated with the EU's push to implement AI border control technologies and the programming and development of AI more generally. The final two sections explore our case study, iBorderCtrl, in part a deception detection and risk assessment AI that 'analyses the micro-gestures of travellers to figure out if the interviewee is lying' (European Commission, 2018). Lying or deception is associated here with risk, which we argue is inherently problematic. Furthermore, the functioning of iBorderCtrl and its lie detection and emotional state analysis functions were designed and based on a small set of mostly European men. This means that iBorderCtrl's functions are both (cis)gendered, raced, and sexualised in the way that they are programmed and likely to be inaccurate or biased towards persons who are not European, (cis)gendered men. As we show, it is both the formulation of iBorderCtrl that is gendered, raced, and sexualised and its practice that assumes that there are universal ways of expressing deception through non-verbal expressions (Sanchez-Monedero and Dencik, 2020, p. 9). Small samples that lack diversity leave AI systems exposed to the risk that their accuracy will fall when exposed to larger, more heterogeneous populations. This can lead to biases that result in AI discrimination and the reproduction of patterns that determine some bodies as more 'worthy of protection' than others (Nayak, 2015). We demonstrate how this can occur, and the negative impacts it has, on two specific groups who may come into contact with AI border control systems: LGBT persons and asylum seekers.

Risk, borders, security

Risk has become increasingly central to the governing of security in the past 20 years. The strategic focus and emphasis of Western governments has generally shifted towards preventive and precautionary logics that inform a range of discrete

practices designed to manage security risks (for example, see Heng, 2006; Rasmussen, 2006; Aradau and Van Munster, 2007; Corry, 2012; Clapton, 2014). This is reflected in several government publications that outline 'risky' strategic environments and specific security risks and their management. In the EU, this includes the 2003 *European Security Strategy* and the recent 2020 *EU Security Union Strategy*. The latter notes that 'Globalisation, free movement and the digital transformation continue to bring prosperity, make our lives easier, and spur innovation and growth. But alongside these benefits come inherent risks and costs' (European Commission, 2020, p. 1). It also highlights 'future-proofing' as a strategic priority, noting that the EU needs to keep pace with evolving risks (European Commission, 2020, p. 6). This focus on security risks is shared by other Western countries, notably the US. The Trump administration's 2017 *National Security Strategy of the United States*, for example, outlines 'reducing risk', 'increasing resilience', and 'improved risk management' as among the key action items of US national security (White House, 2017, p. 14).

Borders and borderlands have become key sites of risk management in Western societies in the last 20 years (Little and Vaughan-Williams, 2017). Vallett and David (2012, p. 112) argue that in this age of risk management following the 9/11 terrorist attacks, borders are back. They have been reinforced, re-emphasised, and bolstered by techno-security apparatuses which focus on surveillance, data-gathering, predictive technologies, and physical barriers, to both manage risk and assure populations that governments are 'doing something' (Vallet and David 2012, p. 114). Preventing risks by keeping undesirables out has led to the implementation of a variety of policies and technologies in the context of managing the risks of terrorism or cross-border crime (e.g. drug trafficking). The Trump administration's travel ban and the construction of a wall along the Mexico-US border are recent and controversial examples of risk management at the border. They are also clear examples of the centrality of race to the othering of immigrants and the characterisation of immigration as a security risk. Trump's presidency is broadly predicated on masculinist depictions of 'strong' and 'decisive' leadership, but more specifically his immigration policy is essentially the securing of White America from racialised and risky others (Fermor and Holland, 2020, p. 56). As Aradau and Van Munster (2009, p. 694) argue, the cultural and racial distinctions upon which othering is predicated are not eliminated, but rather re-inscribed upon processes and technologies of risk management.

These practices serve not only to bring state governing authority to bear on specific geographic spaces within the borderlands, they are also fundamentally embod-

ied. That is, they seek to govern both bodies and borders. The embodied nature of security has been subjected to extensive discussion and critique within the Critical Security Studies literature in the discipline of International Relations (see Ahall, 2018; Waldron and Baines, 2019). Contemporary risk management as a form of security practice, and the employment of data-driven AI within these practices, is also fundamentally embodied. For example, Wilcox (2017) explores drone warfare, algorithms, data, and AI, arguing that drone warfare is both embodied and embodying. As Wilcox (2017, p. 15) suggests, the employment of AI is not a non-human form of decision-making and violence, but rather reproduces gendered and racialised bodies through algorithmic, visual, and affective modes of embodiment. The separation of the perfectible machine and the practices that it enables from humans is problematic, obscuring the operations of race, gender, sexuality, and other signifiers in separating risky from safe and, concomitantly, which populations and which bodies are subjected to sovereign authority and violence and which are not (Wilcox, 2017, pp. 14-15).

Although not writing in this literature, Sanchez-Monedero and Dencik (2020, p. 3) highlight the 'embodied construction of data subjects'. Data is now collected on not only what we say and do online or in other fora, but also on movement, expression, and physiology (Sanchez-Monedero and Dencik, 2020, p. 3). Sovereignty comes to be exercised upon and through bodies (Muller, 2010, p. 12). Borders cease to be solely physical spaces and instead become inscribed upon bodies. This embodiment of risk and its management temporally extends sovereign power into the future. The 'temporal terrain' of risk is not the present, but rather the future, on what might occur. As Puar (2007, p. 185) suggests, 'What is being preempted is not the danger of the known subject but the danger of not-knowing'. This is because the true nature of risky subjects is predetermined—we know who is dangerous and who is not, because certain bodies are taken to represent risk and danger.

As Wilcox (2017, p. 22) argues, 'The construction of certain bodies as threatening is thus less a matter of what is known about them than a desire to make bodies into what we already know they must be'. Rather, the focus is on anticipating, policing, and preventing what risky populations might do in the future. Hence the emphasis on predictive algorithms and AI that enable the surveillance and management of future possibilities. Risk is therefore neither neutral or objective. First, it exists only in discourse and representation, in predictions and imaginaries of events that have not yet come to pass (and might not do so). Second, the identification of security risks is a process of embodied othering and subjectification, bringing into being risky subjects, bodies, upon which state authority and violence is exercised

on the basis of potential. As we show in the next section, the racialised and gendered foundations of security and risk are also apparent when we consider both the programming of AI and the ethical debates regarding its employment.

Gender, sexuality, race and the ethics of AI and border management

The use of automated and computerised decision-making at the border is supposed to increase the reliability and efficiency of border management (Kenk, Križaj, Štruc, & Dobrišek, 2013). The current landscape of AI and other technologies that are in use or active development by Frontex (2021a) is outlined in its recent report on AI-based capabilities that are applicable to its activities. Certain AI based technologies, such as small unmanned drones that employ AI-based object recognition and tracking capabilities, surveillance towers, and automated maritime data gathering and processing, have already been deployed (Frontex Research and Innovation Unit 2021a: p. 22). While some automated decision-making technologies are now in use, the Frontex Research and Innovation Unit (2021a, p. 29) notes that border management and control is a specific activity that is still heavily dependent on border guards and features relatively little automation. Technologies designed to provide Automated Border Control (ABC) have been piloted and Frontex seeks to further build its capabilities in this area. Its desired capability follows the European Commission's (2021b) definition of ABC:

> *an automated immigration control system that conventionally integrates e-gate hardware, document scanning and verification, facial recognition and other biometric verification to facilitate faster processing of travellers on border crossing while enhancing security through the integration of various AI-enabled tools.*

Other significant technologies in development include the European Travel Information and Authorisation System (ETIAS), scheduled for implementation in 2022 (Frontex, 2021b). ETIAS is a travel authorisation system for citizens of states which are able to travel to the EU visa-free. The ETIAS website (2021) notes that while visa-free travel to Schengen area countries is welcome, it also poses security risks that ETIAS is designed to address. Travellers from eligible visa-free countries will be required to apply for ETIAS prior to travel to the EU. The system will access and cross-check a set of databases that provide biometric and other information about travellers, including the Entry/Exit System and Visa Information System (VIS) (Frontex, 2021b). This sort of data gathering and surveillance is a key aspect of managing risk at the border. More significantly in the context of this paper, the

ETIAS website (2021) notes that further AI-driven technologies are being developed to keep Europe safe, including facial recognition and lie detection.

The emphasis on efficiency and security in general border control practices also underpins the techno-strategic (Cohn, 1987) logic that drives the use and implementation of AI in *non entree* practices. For example, Molnar and Gill (2018) offer a human rights perspective on Canada's use of automated decision-making in the refugee and immigration system. The ethical implications of the use of automated decision-making technologies, as Molnar and Gill (2018, p. 1) demonstrate, have 'life-and-death ramifications'. Their concern is that the 'nuanced and complex nature of many refugee and immigration claims may be lost on these technologies, leading to serious breaches of internationally and domestically protected human rights' (Molnar and Gill, 2018, p. 1). This could include bias, discrimination, privacy breaches, and due process and procedural fairness issues (Molnar and Gill 2018, p. 1). Like Molnar and Gill, we perceive significant ethical dilemmas posed by the EU's use of automated technologies at the border and suggest that they augment the EU's capacity to evade its responsibilities under EU, International Refugee, and International Human Rights Law.

Our ethical concerns stem from the ways in which existing *non entree* practices of push backs, carrier checks, and deterrence measures result in an array of harmful gendered and racialised practices that affect refugees and asylum seekers. This brings together two sets of literature: the first, as discussed above, demonstrates the ethical concerns of the use of AI in border management. The second which we now turn our attention to, has demonstrated the ways in which AI reproduces and furthers biases based on race, gender, gender identity, and sexuality. One of the basic issues that underpins bias in AI is that of the demographic profile of AI programmers, engineers and technicians. Who programmes machines and teaches them how to learn? The AI workforce currently does not exhibit much diversity. This is problematic as historically, the lack of representation among those with the means to produce advanced technologies has often had serious and negative consequences for those not represented in their production (Gebru, 2020, p. 253). The concentration of power in few locations and a lack of racial or gender diversity in AI research and production produces forms of systematic discrimation among already marginalised populations (Gebru, 2020, p. 253).

As Collet and Dillon highlight, those involved in designing AI technologies are not reflective of a diverse population (2019, p. 5). There is considerable evidence of the lack of gender and ethnic diversity in the AI research and industrial workforce (Stathoulopoulos and Mateos-Garcia, 2019, p. 5). In terms of gender, recent reports

have found that 80 percent of academics working in AI at leading US universities were men. In industry, 71 percent of applicants for AI jobs in the US in 2017 were men (Stathoulopoulos and Mateos-Garcia, 2019, p. 5). Nor does the current pipeline promise a better balance in the future. Gender and ethnic minorities are still not balanced in STEM subjects at school or university. Diversification of the AI workforce will be vital in order to design and implement technology which is equitable. The implications of gendered and racial imbalances in the AI development sector have serious consequences. For example, numerous studies have demonstrated the ways in which facial recognition systems can misidentify people of color, women and young people at high rates, posing a significant threat to civil liberties (see Klare, 2012; Cook et al., 2018; Grother, Ngan, and Hanaoka, 2019; Learned-Miller et al., 2020). Returning to Collett and Dillon's (2020, p. 5) work, they also demonstrate the ways in which biased data sets amplify gender and racial inequality and project past and present biases into the future. Gebru (2020, pp. 256-257) highlights the problem of 'runaway feedback loops', the process in which the training of AI using past data corrupted by subjective biases only generates further bias and discrimination which then feeds back into the original data sets used to train AI, deepening and increasing the existing marginalisation. Building on this work, we incorporate intersectional feminist theory below to examine the bias embedded in the design and practices of AI technologies at the border. We expect that in bringing these two literatures closer together, we will uncover the ways in which AI reproduces inequalities at the border that are organised through and by the interactions of gender, race, sexuality, and sexual and gender identity.

Introducing the case study: iBorderCtrl

iBorderCtrl represents the latest initiative in a longer and larger attempt by the EU to craft high-tech borders along its periphery. Driven by the logic of data accumulation, the EU's 'smart border' consists of information systems including the VIS, the Schengen Information System (SIS), and the European Asylum Dactyloscopy Database (EURODAC) that operate to control border crossing traffic, migration and asylum applications, and electronic passports (Sánchez-Monedero and Dencik 2020, p. 2). iBorderCtrl is an EU-Horizon 2020 funded project, and invokes the 'smart' border language in its objectives. In the project website it states that iBorderCtrl is Smart 'deception detection' (EU Commission Project Website, 2018). The project involved a number of participants, including several universities, private for-profit entities (excluding Higher or Secondary Education Establishments), and the Hungarian National Police, Latvian State Border Guard, and the Hellenic Police, including Greek border guards (see iBorderCtrl, 2016).

Sánchez-Monedero and Dencik (2020, p. 14) explain that the iBorderCtrl '…project exemplifies the race to AI, the growing industry around biometrics and emotion detection for the purposes of population management, underpinned by a perceived political crisis that has strengthened the rhetoric of border regimes'. In addition to this, COVID-19 has further exacerbated the already limited access to protection and strengthened *non entree* policies and practices. We find this a concerning trend. AI may become more popular as it offers an efficient solution to managing population movements amidst a pandemic. However, the serious consideration that the EU is now giving to the deployment of AI-based border control technologies, combined with the possibility that many of the temporary COVID-19 related measures will 'harden into permanence' (Ghezelbash and Tan 2020, p. 677) suggests that reflecting on the limitations and possibilities of AI technologies is urgent. As Sánchez-Monedero and Dencik also note, there has been a 'lack of transparency surrounding the processes and details of the iBorderCtrl project, including ethical questions and the relationship between the research team and private companies on the project (2020, p. 4).

As a solution, it is posited that iBorderCtrl 'paves the way towards the interoperability of EU systems for security, border management as envisaged by the EC' (European Commission, 2021c). iBorderCtrl proposes:

> *a two-stage process with a pre-registration step to provide traveller information, and a later border crossing stage that includes biometric identification and matching, document authenticity analysis, interaction with external legacy and social systems, an Automatic Deception Detection System (ADDS), a Risk Based Assessment Tool (RBAT) and a post hoc analytics tool* (Sanchez-Monedero and Dencik, 2020, p. 4; also see iBorderCtrl, 2016).

The Periodic Reporting for Period 2 - iBorderCtrl, mentions that, 'iBorderCtrl already implements many of the features planned to be included in the EES and ETIAS Systems both proposed by the European Commission to enhance the border control check procedures' (European Commission, 2021c). Reading through the Technical Framework of the iBorderCtrl project it becomes clear its dual purpose is centered on 'deception detection' and 'risk assessment' in the border-crossing encounter (iBorderCtrl 2016, see also Sánchez-Monedero and Dencik, 2020, p. 4).

iBorderCtrl premises its novelty on the above mentioned two stage process to determine who are *bona fide* travellers (Sánchez-Monedero and Dencik, 2020, p. 4).

Interestingly the Technical Framework also mentions, 'iBorderCtrl is a human in the loop system and the Border Guard will use his/her experience in making the final decision' (iBorderCtrl, 2016). There are two things worth noting about this statement. First, who is the human and what is the loop? Second, it is notable that this statement from iBorderCtrl's Technical Framework refers to a gender dualism (his/her), signifying that the authors of this document conceive of sex and gender as a binary. We return to the significance of this below. The emphasis on the 'human' in the human in the loop (HITL) in combination with the his/her reference, piques our feminist intersectional curiousity, given that to be fully understood as human entails a history of oppression organised through hierarchies of race, gender, gender identity, and sexuality (see Howell and Richter-Montpetit, 2019; Marhia, 2013).

Here though we focus on the issue of who is the human in what loop? HITL is an AI system in which a 'human operator is a crucial component of an automated control process, handling challenging tasks of supervision, exception control, optimisation and maintenance' (Rahwan 2018, p. 6). We can assume that the inclusion of HITL, following Rahwan's (2018) work, fulfils two major functions in the AI system of iBorderCtrl. First, is that humans 'can identify misbehavior by an otherwise autonomous system, and take corrective action' (Rahwan, 2018, p. 7). For example, in the case of weaponised drones, should a computer vision system misidentify a civilian as a combatant, the human operator can override the system and avoid the error (Rahwan, 2018, p. 7). Second, humans can be involved in order to 'provide an accountable entity in case the system misbehaves' (Rahwan, 2018, p. 7). While HITL is considered necessary in AI to include human oversight, we find it interesting that HITL functions on the assumption that the *human* in the loop is capable of distinguishing error and not 'misbehaving' themselves.

In the case of distinguishing asylum seekers from other irregular migrants, for example, there is not enough evidence to convince us that EU border guards do well in this regard and more so, do it without 'misbehaving'. Frontex has recently been accused of complicity in illegal and dangerous pushbacks at sea (Fallon, 2020). The human in the loop may therefore be ineffective (Gregor, Murray, and Ng, 2019, p. 317). Humans 'in the loop' may assume that recommendations based on AI are more accurate or neutral and defer to these recommendations (Gregor, Murray, and Ng, 2019, p. 317). Indeed, this is a significant assumption of the iBorderCtrl project. One of the project's objectives is to 'reduce the subjective control and workload of human agents and to increase the objective control with automated means that are non-invasive and do not add to the time the traveller has to spend at the bor-

der' (iBorderCtrl, 2016). This assumption of machine or AI objectivity compared with human subjectivity reflects an overreliance on technology and ignores the imprinting of the very human subjectivities that iBorderCtrl is seeking to avoid in its programming and use.

Officially the iBorderCtrl project closed in August 2019, and at the time of writing it was difficult to ascertain whether or not iBorderCtrl would be implemented by the EU. There is currently a lack of clarity as to whether or not iBorderCtrl will become a part of the EU's high-tech border. Given the relatively recent end to the project, we find it important to explore the EU's venture into AI border technologies and contribute to criticisms of iBorderCtrl (Sánchez-Monedero and Dencik, 2020; Molnar, 2019) should there be renewed interest to implement this technology. Below, we consider the ways in which the use of AI technologies to manage borders needs to also take seriously the ways in which logics of gender, race, and sexuality configure when AI is used in 'deception detection' and 'risk assessment'.

The gendered, sexualised, and racialised impacts of AI border control

To turn to the ethical concerns we draw upon research in the socio-psycho-legal field that has explored the relationship between credibility, legal judgements, and refugee protection (Rogers, Fox, and Herlihy, 2015; Molnar, 2019) as well as the Critical Security Studies literature that has explored questions of security, ethics, and protection from intersectional perspectives. The argument we build here resonates with Molnar (2019), who describes iBorderCtrl's capacity to become more 'skeptical' through a series of increasingly complicated questions as problematic should an asylum seeker interact with this system. At present it is not envisioned that iBorderCtrl or similar technologies would make refugee status determination (RSD) decisions. However, we find it nonetheless important to explore the potential impact of the increased use of AI at the EU's border, given the recent EU Commission proposal to harmonise the rules on AI in migration, asylum and border control management, as mentioned above . We perceive a number of protection issues that arise should asylum seekers interact with iBorderCtrl, based on the problems and issues identified above regarding its use in controlling regular border flows. What follows here draws from existing research on credibility, refugee protection, gender, sexuality and race and transposes it to iBorderCtrl to imagine what this means for the ethical use of AI and the EU's protection responsibilities.

We develop two interrelated claims. First, AI border technologies can discriminate against persons who have survived trauma and second, that this discrimination re-

produces and exacerbates experiences of trauma, in particular for women, people of color, and LGBT persons. We start with establishing the ways in which trauma and memory interact with AI and refugee decision making and then continue to discuss how this has a potentially harmful impact on people who are more likely to have experienced violence and trauma because of their identity. As Ana Beduschi has highlighted, the increasing reliance on technology to collect personal data could create additional administrative processes that could exclude asylum seekers from protection (2020, p. 6). It is possible the data collected at the border may be used in later asylum claims as evidence that a person either lied or was deceitful in their attempt to enter the EU, which could be used to argue that the person cannot be trusted, their story is not credible, and on that basis their asylum claim denied. This raises a number of ethical concerns if iBorderCtrl cannot account 'for trauma and its effects on memory, or for cultural differences in communication' (Molnar, 2019). Furthermore, 'this use of AI again raises concerns about information sharing without people's consent, as well as about bias in identification through facial recognition, as facial recognition technologies struggle when analyzing women or people with darker skin tones' (Molnar, 2019).

AI technologies like iBorderCtrl are likely to misrecognise (or not recognise at all) trauma and possibly incorrectly detect deception in the vocal patterns, facial movements and microgestures of a trauma survivor. Herlihy and Turner (2015, p. 1) have demonstrated that asylum seekers who have experienced detention and torture are unlikley to have documentation to evidence this; therefore, an assessment of the *credibility* of trauma history forms the basis for decision making. Given that psycho-social-legal research has clearly illustrated that PTSD avoidance symptoms, such as shame or dissociation, are high amongst refugees with a history of sexual violence (Herlihy and Turner, 2015, p. 3), the assumption that asylum seekers are able to fully disclose their traumatic experiences is concerning. It is likely that the use of AI to ascertain credibility will reproduce and possibly worsen the negative impact that has already been evidenced in refugee decision making procedures that rely on human judgement. What has already been established in relation to credibility judgements in refugee decision making (Rogers, Fox, and Herlihy, 2015, p. 149), raises serious ethical concerns should the use of AI be more widely used to determine 'who is worthy of protection' (Nayak, 2015). This suggests to us that the ways in which trauma is gendered, sexualised, and raced presents significant obstacles should refugees escaping these forms of violence come into contact with AI technology designed to detect lies and deception.

We conceptualise gender, race, and sexuality as interacting and interrelated rather

than separate discourses in the following paragraphs. As mentioned, iBorderCtrl's functions are based on the assumption that 'there are universal ways of expressing deception through non-verbal expressions' (Sanchez-Monedero and Dencik, 2020, p. 9). Extending on Sanchez-Monedero and Dencik, there is a large degree of cis- and white privilege embedded in this assumption. Cis privilege is reproduced in the ways in which AI, including iBorderCtrl, is programmed to detect gender as binary: male/female. As Os Keyes (2019) has highlighted, the use of facial recognition technology to 'recognise' or 'detect' gender will hurt trans and gender non-conforming people. When AI is trained to treat gender as a 'binary, immutable and physiologically-discernible concept' it erases transgender people, their concerns, needs and existence from design and research (Keyes, 2019, p. 88.1). Furthermore, as Hamidi, Scheuerman, and Branham have demonstrated, when gender diversity is not programmed into technologies such as iBorderCtrl, the potential for misgendering presents 'severe implications for the mental and physical health of trans individuals' (2018, p. 3). Therefore the potential for harm for gender non-conforming bodies exposed to AI at the border, when a binary logic of gender informs the algorithms at work, is immense.

In addition, the question of credibility and the use of AI to detect lies and deceit also disproportionately affects transgender people and gender non-binary folks. Sjoberg and Shepherd (2012) have established this in relation to the use of body scanning technologies at airports. In this context they highlight the ways in which honesty, lies, and credibility has a harmful impact on transgender people and gender-nonconforming bodies (2012). They write that,

> *Whether a transperson is read as inadvertently deceptive or explicitly described as a liar, the implication for security discourses seems to be the same: someone who would misrepresent themselves (to security personnel) is a risk for (committing terrorist) violence.* (Sjoberg and Shepherd, 2012, p. 18)

While airport security is distinct from border security, translating this research into the context of AI border technologies and iBorderCtrl raises some significant concerns. Namely that if the purpose of AI border technologies is to detect deceit and assess risk, they do so by reproducing cis privilege and exacerbating insecurity for gender-non conforming folks. The potential for violence here is alarming, given that, as Talia Mae Bettcher has demonstrated, the representation of transgender people as deceptive is inherently transphobic (2007, p. 48). As Bettcher explains, the implications for transgender people generally is that they face a double bind.

Either they disclose 'who one is' and come out as a pretender (Bettcher, 2007, p. 50), or refuse to disclose and be a deceiver and run the risk of forced disclosure, the effect of which is exposure as a liar (Bettcher, 2007, p. 50). On one side of the double bind transgender people face having their lives constructed as fictitious, not having their own identifications taken seriously, being viewed in highly condescending ways and being the subject of violence and murder (Bettcher, 2007, p. 50). On the other side of the bind transgender people face 'living in constant fear of exposure, extreme violence, and death; disclosure as a deceiver or liar (possibly through forced genital exposure); being the subject of violence and even murder; and being held responsible for this violence' (Bettcher 2007, p. 50). Transposing the double bind to transgender people interacting with AI border technologies, there is considerable risk that deception detection technology will operate on both sides of the double bind that Bettcher (2007) describes, underscored by the transphobic assumption that transgender people are liars.

The implications of the use of AI to detect lies and deceit for transgender people is alarming regardless of their reasons to travel between states. For asylum seekers who are transgender, the prospect of navigating lie detection AI technologies at borders may mean that they seek alternative, irregular pathways to reach safety, which can be used to characterise their asylum claims as 'abusive' (Moreno-Lax, 2017, p. 5). Therefore the introduction of AI technologies to manage the EU's borders is likely to have a disproportionate and potentially dangerous impact on transgender folks. The use of AI technologies such as iBorderCtrl at the border will likely further exacerbate the already violent impact that *non entree* measures have on LGBT asylum seekers. For example, as Nan Seuffert writes, in Australia, LGBT asylum seekers face discrimination including inappropriate treatment or denial of access to health care and other social services, arbitrary detention, blackmail, extortion and physical and sexual violence (2013, p. 759). These patterns of violence exist across the displacement cycle, however there may be heightened risk for LGBT folks due to fear of disclosing the reasons for flight or fear of authorities in countries of first arrival being unable or unwilling to help (Seuffert, 2013, p. 759). These are contexts that are simply beyond the capacity of AI-based deception detection and risk assessment technologies such as iBorderCtrl to appropriately consider in its decision-making processes. Even with a human in the loop, the risk remains high that interaction with these technologies will further marginalise asylum seekers and transgender people.

Berg and Millbank have argued that the trend in asylum seeker decision making is that claims based on group membership for lesbian, gay, and bisexual refugee ap-

plicants are frequently disbelieved (2009). Given the challenges LGBT asylum seekers already face in establishing credibility, it is worrying to consider what an additional barrier, the use of AI to detect lies and deceit, would mean. It is difficult for LGBT asylum seekers to disclose intimate and personal information which they may have had to hide, or lie about in their countries of origin to stay safe. As LaViolette notes, 'in many countries, repression of sexual minorities is state sponsored or encouraged, so it is difficult for many to imagine that state officials could possibly be anything less than hostile to discussions (2010, p. 195). It is therefore important to consider the ramifications should LGBT refugees come into contact with iBorderCtrl. For example, how does lie detection technology react when a LGBT person may have spent a long time 'lying' about their sexuality as a measure of self protection? Here lying acts to protect, but when it interacts with AI border technologies the self-protection that the lie provides can be undone. Paradoxically, should the 'lie' be detected then any possibility of protection becomes fraught. Credibility and deception, or the possibility to be understood as credible (and therefore not deceptive) relies on gendered and sexualised assumptions.

In addition to gender identity and sexuality, there exists considerable literature identifying the racial assumptions embedded in AI (Lee, 2018; Noriega, 2020). Noriega's study of the use of AI in police interrogations illustrates the ways in which gender and race bias functions in decisions of guilt and innocence (2020). In border technologies, the use of biometric face recognition systems has been described as 'infrastructurally calibrated to whiteness' (Pugliese, 2010). Meaning whiteness is programmed into the algorithmic functions. As Noble has illustrated, "the rhetorical narrative of 'Whiteness as normality' configures information technologies and software designs and is reproduced through digital technologies" (2013, p. 6). What this suggests is that the ways in which race intersects with other identity categories and AI at the border, has serious implications for the assessment of credibility, deceit, and risk. Silverman and Kaytaz (2020, p. 3) note that concepts such as risk, criminality, and legality are overly associated with people identifying with racial, sexual, and gender identities other than those of White, male, cisgender, and heterosexual. Various biases, including race, class, gender, and ableist, inform constructs of risk, criminality, and legality.

Based on research that has demonstrated AI can either be programmed to be racist, or 'learn' and reproduce racism, it is highly likely that iBorderCtrl will extend and reproduce the gendered and racialised construction of risk and threat 'consequentially sustaining the notion of a superior, progressive, white Europe' (Stachowitsch and Sachseder, 2019, p. 108). Furthermore, the very assumption that AI can

help humans overcome their subjective biases is reflected in the idea of a 'superior, progressive, white Europe' that Stachowitsch and Sachseder (2019, p. 108) describe. This is particularly significant regarding asylum claims—the two largest countries of citizenship among first time asylum applicants in 2020 were Syria and Afghanistan (Eurostat, 2021). The potential that asylum seekers arriving at European borders from regions such as the Middle East will be forced to interact with racially biased AI again raises serious concerns regarding the ability of people of colour to have their asylum claims appropriately processed and access protection.

It is clear that there are protection concerns with the implementation of AI as part of the EU's attempt to manage its borders. The use of AI, with the assumption that the management of borders will become more efficient, brings with it heightened risks for survivors of trauma, LGBT persons, and persons of colour to be further marginalised. Using AI as an additional layer to already existing *non entree* measures could mean that these groups are further deterred from seeking asylum or may have to undertake more dangerous, irregular means of migration to reach the EU. While the EU imagines that the use of AI in border management will improve efficiency and security, we envision a future in which current *non entree* measures are reinforced and further intensified with the inclusion of technologies like iBorderCtrl. This is in addition to iBorderCtrl's and other AI border technologies' impacts on regular travellers crossing EU borders. We find the implications of this particularly troubling if we consider the ways in which AI may be programmed to discriminate or misidentify transgender persons, persons of color, or survivors of trauma. Nor are we convinced that a 'human in the loop' will mean that discrimination programmed into AI will be corrected. We also highlighted that the use of AI to detect deception and lies may reinforce the ways in which 'truth' and credibility are organised by white, cis-gendered, heterosexual privileges. We foresee the confluence of 1) the strengthening of *non entree* and *non refoulement* practices during the COVID-19 pandemic (Ghezelbash and Tan, 2020), and 2) the emphasis of the EU on the 'on-discriminatory nature' of AI in immigraiton, asylum and border control as concerning.

Conclusion

In this article we have explored the ways in which the use of AI to detect lies and deceit at the border is likely to reproduce a series of privileges attached to whiteness, cisgender, heteronormativity, and persons who have lived free from trauma. The use of AI in border management needs to take seriously the ways in which algorithms are based on cisgendered, white masculine bodies, which means that not

only their programming is biased, but their application at the border is likely to exacerbate already highly gendered, racialised, and sexualised discourses and practices of risk management, protection and border control. Should the main purpose of AI's use at the borders of Europe be to detect lies and deceit as a way of managing risk, then we should expect this to have a disproportionate and harmful impact on already marginalised persons. Given that evidence exists to demonstrate that the *non entree* measures that do not use AI already have a disproportionate and largely negative impact on survivors of sexual violence, LGBT persons, and persons of color, then we should be very concerned about the possibility of AI to reproduce these patterns and possibly augment them.

The use of AI, as part of efforts to manage risk at the border of the EU, will most likely mean that constructions of risk, lies, and deceit will draw from and reproduce gendered and racialised security logics. The potential impacts of AI border control technologies do not bring about more humane border practices that take seriously the ways in which trauma, violence and protection intertwine with gender, sexuality and race. The trialing and research conducted on the use of AI to manage Europe's borders needs to take these ethical concerns seriously. The EU Commission proposal for a regulation harmonising AI rules on artificial intelligence does note that 'AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position…' (2021a, p. 28). It classifies AI systems intended to evaluate the emotional state of a subject or engage in deception detection in the areas of migration, asylum, and border control as 'high risk'.

While this recognition of the risks associated with AI border control is welcome, there are two major issues here. First, the regulation explicitly excludes most of the high risk AI border control technologies discussed above from the scope of their application. The regulation notes that it will not apply to AI and large-scale IT systems 'in the Area of Freedom, Security and Justice managed by the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA)…that have been placed on the market or put into service before one year has elapsed from the date of application of this Regulation' (EU Commission, 2021a, p. 5). Article 83 further states that the regulation will not apply to AI that is part of large-scale IT systems established by legal acts included in Annex IX of the proposal (European Commission 2021a, p. 87). These include ETIAS, EES, VIS, SIS, and EURODAC. No justification or rationale is given for the exclusion of these AI-powered systems.

Second, the measures proposed for mitigating the risks posed to the fundamental

rights of travellers or asylum seekers emphasise issues such as data set quality, transparency, and human oversight, none of which are necessarily sufficient to overcome gendered, sexualised, and racialised logics without broader social and cultural change (European Commission, 2021a, p. 29). We note that the above measures, or others such as simply increasing diversity in AI development and programming workforces, are unlikely to be sufficient on their own. Rather, this must be embedded within wider structural and cultural reforms that challenge and displace racist, misogynist, and discriminatory attitudes, beliefs, and practices. Further, asking feminist questions in the field of data, technology and protection needs to first unsettle the assumptions placed on the referent object of protection. We also need to ask what it is that requires protection in debates concerning technologies, management, and security.

References

Ahall, L. (2019). Feeling Everyday IR: Embodied, affective, militarising movement as choreography of war. *Cooperation and Conflict*, *54*(2), 149–166. https://doi.org/10.1177/0010836718807501

Amoore, L. (2009). Algorithmic War: Everyday Geographies of the War on Terror. *Antipode*, *41*(1), 49–69. https://doi.org/10.1111/j.1467-8330.2008.00655.x

Anonymous. (2020). *IBorderCtrl automates discrimination*. https://iborderctrl.no/blog:iborderctrl_automates_discrimination

Aradau, C., & Van Munster, R. (2007). Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. *European Journal of International Relations*, *13*(1), 89–115. https://doi.org/10.1177/1354066107074290

Aradau, C., & van Munster, R. (2009). Exceptionalism and the "War on Terror": Criminology Meets International Relations. *British Journal of Criminology*, *49*(5), 686–701. https://doi.org/10.1093/bjc/azp036

Beduschi, A. (2020). International migration management in the age of artificial intelligence. *Migration Studies*, mnaa003. https://doi.org/10.1093/migration/mnaa003

Berg, L., & Millbank, J. (2009). Constructing the Personal Narratives of Lesbian, Gay and Bisexual Asylum Claimants. *Journal of Refugee Studies*, *22*(2), 195–223. https://doi.org/10.1093/jrs/fep010

Bettcher, T. M. (2007). Evil Deceivers and Make-Believers: On Transphobic Violence and the Politics of Illusion. *Hypatia*, *22*(3), 43–65. https://doi.org/10.1111/j.1527-2001.2007.tb01090.x

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*(3), 209–225. https://doi.org/10.1177/0967010614530459

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness* (p. dup;9780822375302/1). Duke University Press. https://doi.org/10.1215/9780822375302

Clapton, W. (2014). *Risk and Hierarchy in International Society*. Palgrave Macmillan UK. https://doi.org/10.1057/9781137396372

Cohn, C. (1987). Sex and death in the rational world of defense intellectuals. *Signs: Journal of Women in Culture and Society*, *12*(4), 687–718. https://www.jstor.org/stable/3174209

Collett, C., & Dillon, S. (2019). *AI and gender: Four proposals for future research*. The LeverhulmeCentre for the Future of Intelligence. http://lcfi.ac.uk/media/uploads/files/AI_and_Gender___4_Proposals_for_Future_Research.pdf

Cook, C. M., Howard, J. J., Sirotin, Y. B., Tipton, J. L., & Vemury, A. R. (2019). Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *1*(1), 32–41. https://doi.org/10.1109/TBIOM.2019.2897801

Corry, O. (2012). Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change. *Millennium: Journal of International Studies*, *40*(2), 235–258. https://doi.org/10.1177/0305829811419444

European Commission. (2018a). *Periodic Reporting for period 2—IBorderCtrl (Intelligent Portable Control System)*. https://cordis.europa.eu/project/id/700626/reporting

European Commission. (2018b, October 24). *Smart lie-detection system to tighten EU's busy borders*. https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders

European Commission. (2020). *Communication from the Commission on the EU Security Union Strategy COM(2020) 605 final*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

European Commission. (2021a). *Automated Border Control (ABC)*. Migration and Home Affairs. https://ec.europa.eu/home-affairs/pages/glossary/automated-border-control-abc_en

European Commission. (2021b). *Proposal for a regulation of the European Parliament and of the Council Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts. COM(2021)/206*. https://eur-lex.europa.eu/

European Travel Information and Authorization System. (2021). *ETIAS & artificial intelligence: The role of AI in border control*. https://www.etiasvisa.com/etias-news/etias-artificial-intelligence-border-control

Eurostat. (2021). *Asylum statistics*. https://ec.europa.eu/eurostat/statistics-explained/index.php?

Fallon, K. (2020, October 24). EU border force 'complicit' in illegal campaign to stop refugees landing. *The Guardian*. https://www.theguardian.com/global-development/2020/oct/24/eu-border-force-complicit-in-campaign-to-stop-refugees-landing

Fermor, B., & Holland, J. (2020). Security and polarization in Trump's America: Securitization and the domestic politics of threatening others. *Global Affairs*, *6*(1), 55–70. https://doi.org/10.1080/23340460.2020.1734958

Frontex - European Border and Coast Guard Agency. (2021a). *Artificial intelligence based capabilities for the European Border and Coast Guard* [Report]. https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf

Frontex - European Border and Coast Guard Agency. (2021b). *ETIAS*. https://frontex.europa.eu/futur

e-of-border-control/etias/

Gammeltoft-Hansen, T., & Hathaway, J. C. (2015). Non-refoulement in a world of cooperative deterrence. *The Columbia Journal of Transnational Law*, *53*(2), 235–284.

Garcia, M. (2016). Racist in the machine: The disturbing implications of algorithmic bias. *World Policy Journal*, *33*(4), 111–117.

Gebru, T. (2020). Race and Gender. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford Handbook of Ethics of AI* (pp. 251–269). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.16

Ghezelbash, D., & Feith Tan, N. (2020). The End of the Right to Seek Asylum? COVID-19 and the Future of Refugee Protection. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3689093

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Hamidi, F., Scheuerman, M. K., & Branham, S. M. (2018). Gender Recognition or Gender Reductionism?: The Social Implications of Embedded Gender Recognition Systems. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3173574.3173582

Heng, Y. (2006). *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*. Routledge.

Herlihy, J., & Turner, S. (2015). Untested assumptions: Psychological research and credibility assessment in legal decision-making. *European Journal of Psychotraumatology*, *6*(1), 27380. https://doi.org/10.3402/ejpt.v6.27380

Howell, A., & Richter-Montpetit, M. (2019). Racism in Foucauldian Security Studies: Biopolitics, Liberal War, and the Whitewashing of Colonial and Racial Violence. *International Political Sociology*, *13*(1), 2–19. https://doi.org/10.1093/ips/oly031

iBorderCtrl. (2016). *iBorderCtrl: Intelligent Portable Control System*. https://www.iborderctrl.eu/

Independent High Level Group Artificial Intelligence. (2019). *A definition of AI: Main capabilities and disciplines*. European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

Kenk, V. S., Križaj, J., Štruc, V., & Dobrišek, S. (2013). Smart surveillance technologies in border control. *European Journal of Law and Technology*, *4*(2). https://ejlt.org/index.php

Keyes, O. (2018). The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–22. https://doi.org/10.1145/3274357

laViolette, N. (2010). "UNHCR Guidance Note on Refugee Claims Relating to Sexual Orientation and Gender Identity": A Critical Commentary. *International Journal of Refugee Law*, *22*(2), 173–208. https://doi.org/10.1093/ijrl/eeq019

Learned-Miller, E., Ordóñez, V., Morgenstern, J., & Buolamwini, J. (2020). *Facial recognition technologies in the wild: A call for a federal office*. Algorithmic Justice League. https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf

Lee, N. T. (2018). Detecting racial bias in algorithms and machine learning. *Journal of Information, Communication and Ethics in Society*.

Little, A., & Vaughan-Williams, N. (2017). Stopping boats, saving lives, securing subjects: Humanitarian borders in Europe and Australia. *European Journal of International Relations*, *23*(3), 533–556. https://doi.org/10.1177/1354066116661227

Marhia, N. (2013). Some humans are more *Human* than Others: Troubling the 'human' in human security from a critical feminist perspective. *Security Dialogue*, *44*(1), 19–35. https://doi.org/10.1177/0967010612470293

McGregor, L., Murray, D., & Ng, V. (2019). International Human Rights Law as a Framework for Algorithmic Accountability. *International and Comparative Law Quarterly*, *68*(2), 309–343. https://doi.org/10.1017/S0020589319000046

Molnar, P. (2019). Emerging voices: Immigration, iris-scanning and iBorderCTRL – The human rights impacts of technological experiments in migration. *OpinioJuris*. http://opiniojuris.org/2019/08/19/emerging-voices-immigration-iris-scanning-and-iborderctrl-the-human-rights-impacts-of-technological-experiments-in-migration/

Molnar, P., & Gill, L. (2018). *Bots at the Gate: A human rights analysis of automated decision-making in Canada's immigration and refugee system*. The Citizen Lab. https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf

Moreno Lax, V. (2017). *Accessing asylum in Europe: Extraterritorial border controls and refugee rights under EU law*. http://rave.ohiolink.edu/ebooks/ebc/9780198701002

Müller, B. (2010). *Security, risk and the biometric state: Governing borders and bodies*. Routledge.

Nayak, M. (2015). *Who is Worthy of Protection?: Gender-Based Asylum and US Immigration*. Oxford University Press.

Noble, S. U. (2013). Google search: Hyper-visibility as a means of rendering black women and girls invisible. *InVisible Culture: An Electronic Journal for Visual Culture*, *19*. https://ivc.lib.rochester.edu/google-search-hyper-visibility-as-a-means-of-rendering-black-women-and-girls-invisible/

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Noriega, M. (2020). The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions. *Futures*, *117*, 102510. https://doi.org/10.1016/j.futures.2019.102510

Puar, J. K. (2007). *Terrorist assemblages: Homonationalism in queer times*. Duke University Press.

Pugliese, J. (Ed.). (2010). *Biometrics: Bodies, technologies, biopolitics*. Routledge.

Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. *Ethics and Information Technology*, *20*(1), 5–14. https://doi.org/10.1007/s10676-017-9430-8

Rasmussen, M. V. (2006). *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge University Press.

Rogers, H., Fox, S., & Herlihy, J. (2015). The importance of looking credible: The impact of the behavioural sequelae of post-traumatic stress disorder on the credibility of asylum seekers. *Psychology, Crime & Law*, *21*(2), 139–155. https://doi.org/10.1080/1068316X.2014.951643

Sanchez-Mondedero, J., & Dencik, L. (2020). The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl. *Information, Communication & Society (Online*. https://doi.org/10.1080/1369118X.2020.1792530

Seuffert, N. (2013). Haunting National Boundaries: LBGTI Asylum Seekers. *Griffith Law Review*, *22*(3), 752–784. https://doi.org/10.1080/10383441.2013.10877021

Shepherd, L. J., & Sjoberg, L. (2012). Trans- Bodies in/of War(s): Cisprivilege and Contemporary Security Strategy. *Feminist Review*, *101*(1), 5–23. https://doi.org/10.1057/fr.2011.53

Silverman, S. J., & Kaytaz, E. S. (2020). Examining the 'National Risk Assessment for Detention' process: An intersectional analysis of detaining 'dangerousness' in Canada. *Journal of Ethnic and Migration Studies*, 1–17. https://doi.org/10.1080/1369183X.2020.1841613

Stachowitsch, S., & Sachseder, J. (2019). The gendered and racialized politics of risk analysis. The case of Frontex. *Critical Studies on Security*, *7*(2), 107–123. https://doi.org/10.1080/21624887.2019.1644050

Stathoulopoulos, K., & Mateos-Garcia, J. C. (2019). Gender Diversity in AI Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3428240

Vallet, É., & David, C.-P. (2012). Introduction: The (Re)Building of the Wall in International Relations. *Journal of Borderlands Studies*, *27*(2), 111–119. https://doi.org/10.1080/08865655.2012.687211

Waldron, T., & Baines, E. (2019). Gender and Embodied War Knowledge. *Journal of Human Rights Practice*, *11*(2), 393–405. https://doi.org/10.1093/jhuman/huz021

White House. (2017). *The National Security Strategy of the United States of America*. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Wilcox, L. (2017). Embodying algorithmic war: Gender, race, and the posthuman in drone warfare. *Security Dialogue*, *48*(1), 11–28. https://doi.org/10.1177/0967010616657947

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

cnrs centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies