Race, technology and the necropolitics of border militarism

Corporate actors profiting from refugee and migrant abuse

Authors:
- Dhakshayini Sooriyakumaran, PhD candidate, RegNet School of Regulation and Global Governance, Australian National University;
- Brami Jegan, campaigner, Stop Deportations to Danger

“Regardless of who has or has not committed crimes, punishment, in brief, can be seen more as a consequence of racialized surveillance.” - Angela Davis (2005)

The role of surveillance in society: social sorting

Whilst some literature suggests that surveillance is simply the capture of personal information, Lyon contends that surveillance is a strategy of social control, and that its purpose is to “influence or manage those whose data have been garnered” (Lyon, 2001). In this way, surveillance functions as a process of “social sorting” (Lyon, 2003), where surveillance capacities are used to collect data, categorise, classify, evaluate and ultimately assign individuals and groups an identity in relation to the normative white (or other dominant race or ethnicity), middle-aged, middle-class, able-bodied, cis-gendered, heterosexual male (Lyon, 2005; Marx, 2005).

Historical accounts of colonisation reveal that surveillance was essential for the classification of people and the control of newly acquired territories (Zureik, 2013). From the 14th to the 19th century, European colonists amassed vast quantities of data on the populations they colonised. The foundations of modern-day biometrics, such as fingerprinting, census taking, map-making and profiling, were refined and implemented in colonial settings (Zureik, 2013). Information gathered via surveillance was used by European governments to classify populations according to innate biological traits, and construct racial hierarchies based on flawed notions of “scientific racism”, both in the colonies and at home (Brown & Barganier, 2018). In Australia, white colonisers used these theories of white supremacy to justify violence such as massacres of Aboriginal and Torres Strait Islander people, land theft, removal of children from families, and erasure of language and culture (Anderson & Perrin, 2008).

Systems of surveillance have been instrumental in creating and reinforcing the social identities, divisions, and hierarchies that shape contemporary society (Gandy 1993; Lyon 2003). This is most apparent in the logics that construct the ‘criminal’. Colonial racial taxonomies formed the basis for the modern study of ‘deviance’, a core concept of the scholarly field of Criminology (Brown & Barganier, 2018). Deviance is based on a “constant division between the normal and the abnormal” (Foucault, 1977) so that groups can be “sorted by levels of dangerousness” (Feely and Simon 1994). Harsha Walia, in her book Undoing Border Imperialism observes that “criminals are never imagined as politicians, bankers, corporate criminals, or war criminals, but as a racialised class of people living in poverty. The word criminal becomes synonymous with dehumanising stereotypes of ghettos, welfare recipients, drug users, sex workers, and young gang members” (2013).

The criminalisation of migration intensified in the aftermath of the attacks of 9/11 in New York and Washington DC (Akkerman, 2016; Lyon, 2003). The construction and reinforcement of race-based categories (Finn, 2005) as a potential threat (for example, Arab and Muslim men) justified a suite of new global counter-terrorism policies, legislation and the strengthened power of police and intelligence forces (Pellerin, 2005).

Surveillance serves as a technique to create and sustain borders through defining the grounds for exclusion and inclusion (Marx, 2005), such as citizenship criteria that determines who does or does not belong as a full member of a nation-state (Lyon, 2005). In addition to the ability to admit or exclude, today surveillants – whether at an airport, a welfare office, or a credit card company – have the responsibility of defining people as normal or deviant, desirable or
undesirable, safe or risky, citizen or threat, healthy or diseased. These definitions have profound effects on the freedom of those individuals (Finn, 2005; Lyon, 2005; Marx, 2005). In this way, surveillance plays a central role in reproducing inequality, creating a hierarchy of access to various social, political, or economic benefits (Lyon, 2005).

Achille Mbembe describes the brutality of borders as an embodiment of “necropolitics”, which he defines as the “ultimate expression of sovereignty… the power and capacity to dictate who is able to live and who must die” (2019). Social sorting, and its power to “kill, to let live, or to expose to death” will remain a central feature of contemporary society and only be strengthened through the development of surveillance technologies (Mbembe, 2019; Lyon, 2005).

Neoliberalisation, growing corporate power and border security

Colonial racial hierarchies were the primary structuring principle of the capitalist world economy which laid the foundation for the lasting rift between parts of the world categorised broadly as Global North and Global South1 (Hoogvelt, 1997).

Global North state and corporate interests have been intertwined since colonisation (14th to the 19th century), however neoliberal economic policy of the 1970s ushered in an era of free trade, open markets, privatisation, deregulation, and an expansion of the role of the private sector (Fraser, 2003).

In the Global South neoliberalisation weakened states through the opening of markets to powerful foreign firms. The US established its position as a global empire through coercing Global South countries to accept development loans channelled through the IMF, World Bank, USAID, and other foreign "aid" organisations. When debts could not be repaid large corporations deployed fraudulent and violent tactics to force Global South states to acquiesce to US political pressure (Ayazi and Elsadig, 2019).

This economic globalisation resulted in the simultaneous tightening of borders (i.e. borders of security), alongside the freer flow of goods, information, and certain persons (i.e. borders of economic integration) (Marx, 2005; Pellerin, 2005). These two analytical logics were linked, as securitised borders occurred in regions where economic integration was moving ahead, largely in the Global North (Pellerin, 2005). Border security measures such as the militarisation of borders, immigration detention and deportation were predominantly targeted at impoverished and colonised communities from the Global South, despite the fact that Global North actors were in part drivers of this mass displacement (Walia, 2013).

Neoliberalisation in the Global North manifested in cuts to, and the privatisation of state-furnished public services, from public utilities, education, and health care, to social welfare, public space, and other services (Ayazi and Elsadig, 2019). The withdrawal of the state from public services further magnified its “law, order and security” function (Lyon, 2005). Today, in a world where media-amplified fear of the racialised ‘other’ is commonplace and where ‘security’ has become a primary political goal (Lyon, 2005), the privatisation of surveillance and policing presents lucrative business opportunities for transnational corporations. The “necropolitics” of border militarisation (Mbembe, 2019) has been increasingly outsourced to corporate entities driven by monopolistic extraction and capital accumulation with ‘limited liability’ for the externalities exploited2.

The rise of virtual borders and digital identification systems

The border security paradigm is underpinned by an insatiable quest for more and better knowledge of risk so that ‘deviants’ can be accurately and efficiently identified (Ericson and Haggerty, 1997). This risk knowledge is gleaned through surveillance practices, which today mean the use of information technologies such as biometrics, Internet of Things (IoT), big data, cloud infrastructures and computer vision (Nieto-Gomez, 2014; Vielhauer, 2017). Borders that “contain, channel, and sort” populations and persons have become virtual, expanding surveillance as a method of

---

1 Global South can also refer to the geography of capitalism’s externalities and subjugated peoples both within and beyond the borders of wealthier countries such as the United States and European nations (Hoogvelt, 1997)

2 The term ‘externalities’ describes the shifting of costs or benefits outside of the market. For example, when a company pollutes the atmosphere with carbon dioxide (e.g. Standard Oil), it is the environment and communities of people who experience the impacts of climate change. The company pays nothing for the free use of the atmosphere (Economic Opportunity Institute, 2010).
formalised social control (Lyon, 2002; Lyon, 2005). The automation of border policing further exacerbates the criminalisation of marginalised persons and groups.

Digital identification systems typically combine biometric identifiers, such as fingerprints, facial patterns, iris scans, or voice recordings, with other Personal Identifying Information (PII) for greater accuracy of verification or identification. Increasingly, the body — or information collection about the body — becomes a passport, that both enables and inhibits movement within a given territory and across borders (Lewis, 2005; Muller 2004; Zureik 2004).

Despite the fact that Europe’s General Data Protection Regulation (GDPR) strictly prohibits the processing of biometric data for the purpose of uniquely identifying a person, unless the person gives explicit consent (Article 9, GDPR; Electronic Frontier Foundation, 2020), biometrics are a fast growing industry. The global biometric systems market is forecast to grow from $33.0 billion in 2019 to $65.3 billion by 2024 (Markets and Markets).

A controversial example of the use of biometrics is the Vehicle Face System pilot on parts of the US-Mexico border that records images of people in vehicles crossing the border, with the aim of creating a facial recognition system that checks collected images against those stored by authorities (Brandom, 2018). The more commonplace and seemingly harmless example is biometric data collection at airports. Peter Adey argues that the “airport is now a surveillance machine – an assemblage where webs of technology and information combine” (Adey, 2004). IBM’s multiple contracts with the Australian government, listed below, demonstrate how various datasets can be combined and analysed for risks:

- Department of Home Affairs contract to manage back-end systems that hold personal information collected by departures SmartGates at Australian airports (Office of the Australian Information Commissioner, 2018);
- Department of Home Affairs contract that utilises IBM’s Watson platform to examine useful information hidden in unstructured data sources such as news feeds and government reports (Chanthadavong, 2015);
- Australian Customs and Border Protection Service (ACBPS) contract for an advanced passenger analysis system that “collects and stores Passenger Name Record (PNR) data which is then risk assessed in combination with other relevant information” for the purpose of “identifying travellers who may be a risk ahead of or during travel” (IBM, 2013).

Smart ID cards represent a significant development in surveillance as they introduce a further level to the virtual border of the nation state. Their stated purpose is to give citizens automated access to public services. Yet their true intent is immigration control, fraud control, anti-terrorism, and more efficient policing (Lyon, 2005; Privacy International, 1996). With the widespread adoption of national ID cards, the experience of otherness becomes steadily more ubiquitous, no longer limited to physical borders (Lyon, 2005; Privacy International, 1996). Increasingly, the “border is everywhere” (Lyon, 2005).

The Indian government has introduced the Aadhaar, a randomly generated 12-digit digital ID that was made mandatory for accessing state benefits, welfare subsidies, and to file taxes. When registering for Aadhaar, people are required to share fingerprints and iris scans, in addition to their name, date of birth, gender, address and a facial photograph. Paytm with Aadhaar has also become compulsory. For trans people, who have restricted job opportunities, sex work is often one of the few options available. Under Indian law, both soliciting and living off the income of sex work are crimes. Due to data on payments being linked to data on gender, Aadhaar can inadvertently make sex workers more visible in a way that puts them at risk, placing an already marginalised group under further scrutiny (Kovacs, 2020).

‘Internal’ IDs are likely to be closely tied to the ‘external’ IDs such as passports. In the UK, for example, ID cards are associated with passport and driver’s licence renewals. Consequently, personal data becomes globalised. Technology corporations and governments promote high-tech ID options rather than low-tech, labour-intensive alternatives, as they present an opportunity to secure a monopoly over the means of identification (Lyon, 2005).

Governments around the world are taking steps to connect databases to make them inter-operable. For example, the Council of the EU adopted regulations to enable interoperability between various information systems, including its migration databases, to ‘improve security, allow for more efficient checks at external borders, and contribute to

---

1 Paytm is an Indian e-commerce payment system and financial technology company.
combating illegal migration’. This has led to the development of a European search portal and a shared biometric matching service, which allows the EU and member states simultaneously to search multiple databases and cross-check identities with biometric data (Council of the EU, 2019; Akkerman, 2020). This linking of once-discrete information systems into networks of information means it can be used to generate and analyse information for purposes not even remotely close to the original purpose of information collection (Lyon, 2005).

The most alarming technological development in surveillance societies is the use of these ever-expanding and interconnected data sets, commonly referred to as big data, for predictive policing. Using computational methods, such as Machine Learning (ML), a computer system can learn intelligent behaviour from data (i.e. Artificial Intelligence) and make predictions about the future based on algorithms. Typically, a large part of a data set is used as training to make the system learn, and then it can be used to make predictions based on other data (Gerritson, 2020).

An example of this is the Suspect Targeting Management Plan (STMP), a secret New South Wales (in Australia) policy concerned with deterring the future criminal activity of both recidivist offenders, as well as those who have not been found guilty of offences (but are suspected to be at risk of committing crimes). The STMP includes a quantitative risk assessment tool that uses algorithms to assess the ‘risk’ level of individuals. Identified individuals are subject to a ‘targeted program’ by police officers which includes regular visits to the individual’s home and using police powers such as stop and search. Independent research into the initiative revealed that children as young as nine have been targeted, and that more than 50% of those targeted are Indigenous (Sentas & Pandolfini, 2017).

The trend towards interconnected and expanding big data increases the scope for pre-emptive surveillance (Lyon, 2001; Marx, 2005). This further extends the access of the state and corporation into the lives of those with marginalised identities, defining their futures based on biased datasets and algorithms.

**COVID-19: Surveillance technologies for public health, social welfare, and border policing**

Since the emergence of COVID-19, several countries, including Australia, China, India, Israel, Singapore, South Korea, the US and UK, have deployed invasive digital surveillance to track the spread of the virus and enforce lockdown and quarantine policies. These include the collection of security camera footage, mobile phone location data, bank records, and using facial recognition (Amnesty International, 2020; Manokha, 2020).

In a short period of time health status has become deeply embedded in mobility infrastructure in ways that cannot be easily reversed. The International Centre for Migration Policy Development (ICMPD) envisions a future where “a medical certification and medical card containing information about the current health status and health history will probably be required when travelling” across borders (Eržen et al., 2020; Akkerman, 2020). The computerisation of medical records in recent years has created an abundance of accessible and sensitive information (van de Ploeg, 2002). The pandemic may mark the beginning of a new era of generalised surveillance based on biometrics and health-related big data, where disciplinary control usually reserved for ‘deviants’ is diffused throughout society (van de Ploeg, 2002).

Enhanced corporate interest in the provision of health and policing services as part of the government responses to COVID-19 represents a further blurring between data collected for state and commercial purposes, and another step toward the globalisation of personal data. During a meeting with the UK government, companies with experience (and large government contracts) in border control, such as Palantir, Google, Amazon and Microsoft, discussed “what they could do to help model and track the disease and the impact of government interventions” (Volpicelli, 2020; Akkerman, 2020)).

Modern technology corporations (such as Amazon, Microsoft, and Google) are markedly different to monopolies of the past due to their ability to use vast amounts of data to dictate consumer behaviour, undermine democracy (Zuboff, 2019), and automate security and policing. This centralisation of power and wealth has been thus far largely immune to regulatory interventions, despite ongoing antitrust scrutiny (McLaughlin & Brody, 2020).

---

1 ICMPD is an international organisation, with 18 European states as members, that is focused on combating irregular migration, border management and refugee returns. It works closely with the EU.
Palantir, a company with a history of secretive contracts with military and security actors, is working with at least twelve governments on responses to COVID-19 (Akkerman, 2020). The rise of public-private partnerships between governments and technology companies to combat COVID-19 serves to emphasise the role of the government as ‘client’ and undermines its ability to function as an independent regulator of the technologies deployed (Akkerman, 2020).

**Escalating climate impacts and the militarisation of borders**

Like the pandemic, climate change is another global emergency that is likely to further accelerate the militarisation and surveillance of borders. Climate change contributes to migration and displacement of people by causing more intense or frequent natural disasters, warming and drought, or sea level rise. It is unlikely that climate change is the only reason why someone will be forced to move to seek safety. People displaced by the impacts of climate change are also often displaced by other environmental, economic, political, and social factors.

Political situations and economic conditions are also deeply embedded in the environment. Any environmental disruption has immediate economic or political consequences (Gemene & Zickgraf, 2019). For example, environmental changes can create or exacerbate conflict, displacing more people. This movement of people to ensure their basic needs are met has already begun (Narahari, 2019; Ruppel, 2014).

While much of the initial displacement is occurring within borders, there will inevitably be increased movement across international borders (Lustgarten, 2020). Formal pathways for climate-induced migration are severely underdeveloped and unlikely to improve given the lack of international cooperation. The Global Compact for Safe, Orderly and Regular Migration (GCM) adopted in 2018 recognises climate migration, however, it is based on political promises rather than legal obligations.

Over the past decade climate change has been cast as a national and international security issue (Hayes, 2015). As described by Hayes and Buxton in their book, *The Secure and the Dispossessed: How the military and corporations are shaping a climate-changed world*, “by portraying people as some kind of Hobbesian mass that will inevitably meet food shortages with violence, or as hordes of would-be migrants massing at our borders, we are giving succour to the security strategists and politics of fear that make people more willing to contemplate giving up their freedoms” (Hayes & Buxton, 2015). This framing of climate induced-migration serves to reinforce the construction of race-based categories as a threat, and justify the implementation of increasingly draconian migrant and refugee policies by Global North governments. Walls, bullets, drones and cages are therefore positioned as essential to eliminating this ‘threat’ (Miller, 2019).

As the climate emergency worsens, the border, as a tool of social sorting, will be used by Governments and corporations to categorize populations into those who can be sacrificed and those who must be protected as economies start to fail and resources become scarce. The automation of border policing and the expansion of digital identification systems will make the brutality of borders more efficient; with greater speed, scale, accuracy, and lower cost.

**Lobbying and political donations**

Lobbying and political donations increase the risk of ‘corporate capture’ through which “an economic elite undermines the realization of human rights and the environment by exerting undue influence over domestic and international decision-makers and public institutions” (ESCR, 2020; Akkerman, 2020). This is particularly a risk when ties become too close via the ‘revolving door’ between public office and private companies, that is common in the military and security industry as well as at consultancy companies (Nielsen, 2011; Smithberger, 2018; Zibel, 2019; Chamberlain, 2019). Todd Miller notes, for example “almost all former CBP commissioners and DHS secretaries have shuffled into the private sector or various consulting companies, giving both ‘expert opinions’ and greasing the wheels between industry and homeland security” (Miller, 2019).

---

5 Information in this section has been, in part, drawn from an unpublished Transnational Institute (TNI) report that focuses on key companies and investors involved in immigration detention, transportation and deportation, border policing, technology enabled surveillance and monitoring.
Donations to political candidates, elected politicians and political parties can serve as a means to ‘buy’ influence and to enable companies to secure contracts and policy changes. Research suggests that political donations at the minimum give donors significantly greater access to policymakers (Kalla & Broockman, 2016).

The expanding power of the private sector under neoliberalism is also made manifest through industry lobby groups that seek to influence government policy and procurement processes. These organisations play a role in perpetuating the narrative of migration as a security problem and/or threat, which leads to policies such as increased border security, externalization and privatized immigration detention.

For example, the Security Identity Alliance (SIA), founded by biometrics companies Gemalto (part of the weapons company Thales) and IDEMIA, is an active lobby group in Europe on digital identities. The group recently published a paper titled *Strong identity, strong borders*, which is described as a ‘best practice guidance on the development of a cohesive and effective eBorder strategy’. In it, the SIA explicitly argues for “exporting the border” through interventions before people leave for their destination, for example with a “face to face interview by a representative of the destination country”, including “biometric enrolment - of face and fingerprints for example - which can be checked against police and immigration records back in the home country” (Secure Identity Alliance, 2017). Corporate capture of government policy is a major impediment to effective regulation of emerging technologies.

**Mapping corporate actors involved in the surveillance and militarisation of borders**

Recent market research reports expect an annual growth of the global border security market between 7.2% and 8.6% to a total of 65-68 billion dollars in 2025 (Global Reports Store, 2019). In the US, the budget for border and immigration control has increased by more than 6000% since 1980, demonstrating industry growth under neoliberalism (Miller, 2020).

Industry sectors related to immigration and border management include border monitoring services, transportation of migrants, screening and/or determination of claims for protection, processing of visas and/or pre-departure screening at airports, management and security of immigration-related detention facilities; deportations and returns, collection of biometric data and use of private security technologies to support immigration and border management procedures; security in humanitarian settings (including camps, shelters etc) (UN Working Group on the Use of Mercenaries, 2020). This group of sectors has various definitions. Journalist and author Todd Miller terms the confluence of border policing, militarisation and financial interest as the ‘Border Industrial Complex’ (BIC). Alternatively, the American Friends Service Committee (AFSC) uses the description ‘companies involved in the militarization of borders and the policing of immigration’.

AFSC, the Transnational Institute (TNI), Mijente, Privacy International, Migreurop and other not for profit organisations have been researching the main companies (both private and state controlled) providing these services. For example, AFSC has an extensive divestment list and Mijente’s ‘No Tech for Ice’ campaign research companies that are building the tools used to surveil, incarcerate, and deport communities from the US.

Researchers have also been tracking the asset managers most heavily invested in the companies operating in these sectors. For example, *The Political Economy of Entry Governance* (Lemberg-Pedersen, Hansen, Joel Halpern, 2020) notes “representing free-floating private equity, the Vanguard Group is the top shareholder of 3M, HP, IBM and Accenture, while also owning smaller portions of shares in Airbus, Leonardo, Thales, Safran and Atos. Through its ownership, the Vanguard Group thus dominate a number of companies, which have been central for the construction of the EU databases controlling entry governance, whilst also exercising lesser influence on the companies involved in EUROSUR. Similarly, different BlackRock funds own large numbers of shares in 3M, HP, IBM, Accenture, Safran, Indra, Thales”.

Further to this, Transnational Institute (TNI) will be releasing a report in December 2020 that identifies the financial investors in the key companies in the BIC, the trends shaping its growth and the influence of BIC lobbyists on government policy towards refugees.
References


https://weblog.iom.int/intergovernmental-panel-climate-change-ipcc-calls-more-attention-human-mobility/


https://www.amazonaws.com/arena-attachments/770323/6a088e6a4baa083e1f720982c0b6f8b9.pdf


https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2020/


https://thenewenquiry.com/carceral-capitalism/


https://www.redpepper.org.uk/colonial-oversight/