B Kieran, FA Cascales, L Thomi & M Veit 'Are smart walls smart solutions? The impact of technologically-charged borders on human rights in Europe' (2019) 3 *Global Campus Human Rights Journal* 173-209
http://dx.doi.org/10.25330/483

Are smart walls smart solutions? The impact of technologically-charged borders on human rights in Europe

Bronagh Kieran, Fuensanta Amoros Cascales,***
*Laura Thomi*** and Meredith Veit*****

Abstract: *This article reviews new technologies on the external border of the European Union, and the human rights ramifications of these developments. It utilises a multi-disciplinary approach, writing on the emerging technologies themselves, their impact on vulnerable groups, legal developments relating to privacy, and the political context informing migration policy. The first part outlines emerging trends in border technology. The discussion relies on examples beyond the European Union to inform its analysis, including case studies from the United States border with Mexico. Technological developments considered include thermal imaging; biometric data; virtual reality; artificial intelligence; and drones. The second part explores how vulnerable groups will be affected by the collection of biometrics at the external border of the European Union. This part explores how algorithms, far from being objective arbiters, in fact are repositories for the bias of the manufacturer. The article postulates that to tackle the proliferation of bias, it is necessary to have a diverse workforce creating these systems. Third, the article addresses the regulatory framework on data privacy in the European Union. The significance of a right to privacy post-9/11 context is described. The conception of data privacy of the General Data Protection Regulation (GDPR) is set out. This part first analyses how GDPR has affected the processing and storage of data in the EU and, second, draws out the implications for the data of migrants. Special emphasis is placed on the concept of consent, and the ability of migrants to refuse the collection of their data is put into question. Finally, the article turns to the political context. Arguing that right-wing populism is not inherently opposed to new technologies, the article points to populists' reliance on social media to garner support. Furthermore, it is advanced that the potential for migrants' human rights to be impinged by new technologies is compounded by the influence of right-wing populism on migration policy.*

Key words: *smart borders; surveillance; consent; privacy; biometrics; human rights; vulnerable groups; securitisation; technology; artificial intelligence*

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. BCL Law with Philosophy (University College Dublin) MA in Human Rights and Democratisation (Global Campus Europe).

** BA Law (Universidad de Alicante) MA in Human Rights and Democratisation (Global Campus Europe).

*** BSc in Social Work (Lucerne University of Applied Sciences and Arts) MA in Human Rights and Democratisation (Global Campus Europe).

**** BA in Communication and Public Culture (George Washington University) MA in Human Rights and Democratisation (Global Campus Europe).

1 Introduction

Since the end of World War II a significant number of border walls and fences have been erected around the world as a means of separating the in-group from the out-group. Metal, wire or concrete walls separate Greece from Turkey, Turkey from Syria, Spain from Morocco, Morocco from the Western Sahara, Hungary from Serbia, Israel from Egypt, Israel from the West Bank, Saudi Arabia from Iraq, Iraq from Iran, Malaysia from Thailand, Zimbabwe from Botswana, the United States from Mexico, Pakistan from India, India from Bangladesh, North Korea from South Korea, and the list continues. The European Union (EU) has over 1 000 kilometres of fences or walls guarding member states against non-member states, according to a recent study by the Transnational Institute (Ruiz Benedicto & Brunet 2018). In the 1990s the EU had two walls, while in 2019 there are now 15 walls (Ruiz Benedicto & Brunet 2018).

Since the 9/11 attacks in 2001, the construction of these physical barriers has spiked even further, as leaders preach the imperative urgency – even as a national emergency – of keeping migrants out and nationalists in, furthering a xenophobic 'us versus them' mentality. Governments seemingly build these walls with the unrealistic expectation that they will render their citizens impervious to the effects of any hardship beyond their barbed wire limits. However, as the opposition argues, they are a medieval solution to a twenty-first century problem. As we shift from emergency-driven policies to intelligence and risk management policies, many populist leaders currently in power are offering walls as the simple solution to complex immigration challenges. With this shift to risk management policies, which focus on prevention to obtain the maximum security, proportionality tests should be carefully made since civil rights and liberties could be at stake.

Populist rhetoric revolves around state identity and the consolidation of state sovereignty. This is often tied to an anti-immigrant agenda, whereby immigration is blamed for citizens losing control of their country. In this sense, border walls are emblematic of the populist conception of sovereignty. The militarisation of borders and border walls also feeds into an extremist narrative of state sovereignty, as it implicitly reinforces the divisive rhetoric which portrays immigrants as 'invaders'.

Offered as an alternative and more rational solution, many politicians of the developed world propose intensifying the role that technology plays in determining who can cross over from one state into the next. This article explores the advantages and disadvantages of building digital walls. It examines possible human rights benefits of border technologies, but argues strongly in favour of necessary precautions for integrating innovations from the Fourth Industrial Revolution[1] into states' immigration processes and systems. As technology evolves, it seems that the watchful eye of governments can be overreaching: collecting data without consent, peering over state lines, and treating civilians as suspects.

[1] According to Prof Klaus Schwab (2016), founder and executive Chairperson of the World Economic Forum, the fourth industrial revolution involves imbedding technology into people's everyday lives, and even into their bodies, made possible by advancements in biotechnology, the Internet of Things (IoT), artificial intelligence, robotics, nanotechnology, quantum computing, and more.

But the application of technological advancements can reap true benefits if implemented with a human rights framework in mind. State sovereignty is also affected by technologically-established frontiers in so far as they grant the state additional access to – and, potentially, control over – personal data. This article explores the most advanced technologies being used at the border and plans for future technological integration at transit checkpoints. In analysing topical case studies, the current legal framework and the overall political environment, we aim to critically review how travellers' human rights are being (and potentially could be) impacted.

Moreover, while these technologies redefine the concept of border, they also reaffirm it. Tangibly crossing the border can now involve more than just treading over a single 'line in the sand' and passing through an immigration checkpoint. Now, the areas surrounding the border also include surveillance technologies associated with border control and potentially cause even further human rights violations, particularly considering the effects on vulnerable groups. This is linked to the so-called militarisation of borders. In this way, even where physical walls are not built, strong barriers 'protecting' the state from immigrants may nonetheless be constructed from 'smarter' materials. Security concerns are regularly conflated with questions surrounding immigration policy and the technology it hires. However, this creates a false dichotomy between human rights for immigrants and national security.

The tendency to move towards a 'surveillance society' has also produced a significant shift in citizens' perceptions of both personal privacy and security. As populist discourses in Western societies foster a 'culture of fear' and 'overprotection', so too does the notion that in order to have security, one must relinquish one's privacy. Within this privacy-for-security trade-off, infringements upon privacy and other human rights arise, and along with them questions about the compatibility of constant border surveillance with democratic societies.

Indeed, a pressing problem is political rhetoric that positions migrants as a serious risk to national security, regardless of a connection with arms or human trafficking, drug smuggling, or terrorist activity. This inherently threatens the idea of maintaining human dignity, even more so at the hands of intelligent machine intervention. Security concerns are being paired with a strike against 'illegal' migration,[2] as wars in the Middle East and gripping economic distress and violence in Central America have forced migrants from their dangerous and impoverished nations towards the Western world. In 2015 and 2016 Frontex, the European Border and Coast Guard Agency (nd) detected more than 2,3 million 'illegal crossings'. Refugees are widely considered to be the new 'threat' and anti-immigrant rhetoric is fuelling the desire for states to close their borders, which will be further discussed in part 6 of this article.

Furthermore, the use of more advanced technology attempts to reconcile two aims of the state that are often contradictory, namely, 'facilitating the movement of people while increasing the level of control

[2] Based on legal terminology, 'illegal' immigration occurs when a person crosses into a state's territory without permission from the government. For the purposes of this article, we will refer to mass migration movements as irregular migration so as to not further stigmatise the affected groups.

over them' (Koslowski 2011). This causes tensions between the freedom of movement as well as rights to privacy and security. Security-privacy tradeoffs and the effects of border digitisation on data security and privacy protection will be examined in part 5 of this article.

Finally, scholars have long declared the necessity of integrating ethics and human rights considerations into the development and use of advancing technologies (Bowling, Marks & Murphy 2008: 41). Part 4 of this article argues that greater attention should be given to how furthering the capacities of 'virtual fences' and 'smart borders' impacts all people, regardless of nationality or side of the border, particularly those considered most vulnerable. First, however, the next part sketches the historical development of border technologies, before part 3 provides an overview of state of the art of digital borders.

2 Background and historical development of border technology

Physical borders have traditionally 'marked the limits of sovereign territory and acted as the primary site of expression of the exclusionary powers of the state' (Pickering & Weber 2006: 19) determining who and what should be allowed to cross onto domestic soil. Yet while globalisation intensifies, so does the flow of people, goods and conveyances across geographic lines, making maintaining territorial sovereignty an ever-daunting challenge for border-control authorities (Koslowski 2011). Over the past three decades, substantial increases in funding, staff and technological capabilities used towards surveilling states' air, land and maritime frontiers have amplified political contention over the most efficient and effective ways to maintain a national stronghold (Koslowski 2011). While many specialists argue for a multi-pronged approach to security (Meyers 2003; Mittelstadt et al 2011) deploying more advanced technology – more specifically in the form of algorithmic additions, Internet of Things (IoT)-based information systems and biometrics – is widely considered the 'magic bullet' solution to filling the problematic gaps left by solely erecting physical barriers (Ceyhan 2008: 19; Marx 2005: 9).

As technology evolves, so does its varied applications. However, states that are employing these new technologies for border control purposes cannot be absolved from their responsibility for the resultant human rights implications, regardless of geographically-imposed boundaries. Katja Franko Aas (2005: 22) argues that 'contemporary technological paraphernalia ... not only enables fortification of the border, it also reshapes the border according to its own logic', meaning that a concrete definition of a border can no longer be accurately drawn on any map. The expansive reach of technological capabilities can extend miles beyond any previous understanding of nation-bound jurisdiction.

2.1 The evolution of technology at international transit-points

From the 1970s until the present, states have been using surveillance technology in order to 'make visible the invisible' in terms of politically-determined threats (Haggerty & Ericson 2000: 620). Initially, states installed portable electronic intrusion-detection ground sensors and low-light video cameras at their borders in order to better monitor migrants and traffickers on the ground (Koslowski 2011). However, the equipment lacked effectiveness as it was difficult to determine whether the person or thing that triggered the sensors actually was a threat. Additionally, the video quality on the low-light cameras was extremely poor. At airports, an identity document typically was not required for air travel. Airlines, being generally opposed to conducting individual screenings according to company policies, merely requested suspicious passengers to pass through a metal detector (Gardiner 2013). In the 1990s all metal items were subject to screening through an X-ray machine in search of weapons, and passengers' checked bags were usually only screened on international flights (Gardiner 2013). At this time, certain state borders were more equipped with motion, infrared, seismic and magnetic sensors in order to collect a clearer image of who or what was approaching state lines. By 2000 the United States government had placed approximately 13 000 ground sensors along the US-Mexico border (Gardiner 2013). As camera quality improved, the addition of images and sensors made it possible to determine how many people were on the other side of the border, where they were moving and in which direction, as well as whether or not they were carrying weapons.

Since 9/11 the US has led the global trend of thickening borders, making them less porous and more deflective. Following the attacks, the Transportation Security Administration (TSA) was created in 2001 and the US Department of Homeland Security (DHS) was created in 2003; the DHS quickly began 'including increased manned aerial assets, expanded use of unmanned aerial vehicles (UAVs) and next-generation detection technology' (2005) on US borders. TSA soon commissioned new full-body scanners within all international airports (Arnold 2010). A globally-piercing societal fear which revolves around an imagined 'low probability, high consequence' event is just one consequence of terrorism (Amoore 2013: 11), and national borders and immigration checkpoints have become physical spaces where citizens can tangibly understand the management of catastrophic risks.

Governments introduced data-collection mandates and heightened security screenings in order to create databases of biographic, immigration, and criminal histories of individuals, which are now 'shared among law enforcement agencies in a fashion unprecedented before the 2001 terrorist attacks' (Chishti & Bergeron 2011). The US signed bilateral Smart Border Declarations with Canada and Mexico in December 2001 and March 2002, respectively, calling for the standardisation of biometric data processing for all types of travellers – tourists, migrants and refugees included (Meyers 2005: 14). Immigration policy around the world is now based on information sharing between intelligence agencies as well as international, state and local law enforcement, all of which are increasingly reliant on the latest technologies to collect this data (Mittelstadt et al 2011: 5-9).

Countries around the globe have invested billions of taxpayer dollars into information technology-based programmes such as the Secure Border

Initiative (SBI);[3] the Electronic System for Travel Authorisation (ESTA); automated biometric entry-exit systems such as US-VISIT and Europe's EES; registered traveller systems such as NEXUS, Global Entry and SENTRI; Electronic Travel Information and Authorisation Systems (ETIAS); the Schengen Information System (SIS II); and more (US CBP nd). Government budgets for border control are ballooning under the justification of mitigating alleged national security breaches. The EU announced its €34,9 billion spending plan for 2021 to 2027 on border infrastructure including scanners, automated licence plate recognition systems, and mobile laboratories, as compared to €13 billion from the previous period (European Commission 2018b). Meanwhile, the European Commission (2018a) announced their support towards EU agencies managing security, border and migration management, valued at €14 billion, in comparison to the €4,2 billion from the previous session. The US has spent approximately $41 billion for border security since 2001 (American Immigration Council 2017) and President Trump's proposed wall would cost upwards of $5,7 billion to complete (Nowrasteh 2019). According to Jean-Claude Juncker, President of the European Commission, '[b]etween now and 2027 we want to produce an additional 10 000 border guards. We are now going to bring that forward to 2020' (Angelescu & Trauner 2018). The US Immigration and Customs Enforcement (ICE) has more than doubled in size since President Trump took office (Politifact at the Poynter Institute 2017) and now employs more than 20 000 law enforcement and support personnel.

In 2016 the United Kingdom and France concluded a deal to construct a £2,3 million wall preventing refugees from entering French ports and boarding transport vehicles bound for the UK. The project requires an additional £44,5 million for additional fencing, closed-circuit television (CCTV) surveillance and other detection technology (Travis & Stewart 2018). In India, the Minister of State for Home Affairs, Kiren Rijiju, announced in 2018 that 'a pilot project for deployment of Comprehensive Integrated Border Management Solution (CIBMS) which includes different types of sensors, radars, day and night vision cameras, etc, has been taken up' to prevent the 'infiltration' of foreign threats into Indian territory (The Economic Times 2018). Brazil, too, announced in 2013 its plans to construct a $13 billion virtual wall that will stretch 10 000 miles across 10 border countries, citing the need to curb illicit activities (Moura & Garcia-Navarro 2013). According to predictions by the market research company Frost and Sullivan, the global border protection and biometrics market is projected to grow from $16,5 billion in 2012 to $32,5 billion by 2021 (Ring 2013). Border security and immigration enforcement funding has an ever-increasing budget which is, at least partially, spent on cutting-edge equipment, as further explored in the next part (US ICE 2018; EOP 2019).

[3] In 2006, the United States government commissioned Boeing to create a 'virtual wall' along the southern border, but the project was completely terminated in 2011 after being deemed a failure by the Government Accountability Office: '[a]bout 1,300 SBInet defects had been found from March 2008 through July 2009, with the number of new defects identified during this time generally increasing faster than the number being fixed — a trend that is not indicative of a system that is maturing and ready for deployment.' Around $1 billion had been spent on the project by the time it was cancelled (U.S. GAO, 2010).

3 Constructing digital walls and data-driven barriers

Technology is neither inherently good nor bad, and its simultaneous ability to both cause problems and solve them is what provokes antithetical feelings of awe and apprehension. Arguing for whether or not technological advancements bring about more harm than good is rooted in the effects of their applications, but the full extent to which governments are implementing new technologies for securitisation remains unknown. Behind the semblance of national security, certain research and development initiatives as well as the scope of civilians' data utilisation are kept secret. What the public understands is based on the information they are allowed to know via government press releases, company reports from technology suppliers and developers, investigative reporting, and eyewitness or experiential testimony. The full picture is incomplete, but the evidence that has been disclosed thus far is unfavourable from a human rights perspective.

However, this is not to say that the technologies described in this part are not useful for protecting civilians from legitimate threats, such as violent actors or destructive weaponry, and the aim is to vilify neither border patrol nor the military. To date, it would seem that border technologies are not being applied with a human rights-bound mission in mind. Technology that has otherwise been used in wartime now is targetedly aimed at migrants, and the consequences of unquestioned civilian surveillance are already apparent along EU and US borders.

3.1 Technologies currently in use at the border

While steel fences and concrete walls lined with barbed wire continue to be erected around the world, military contractors are leading the armament of traditional border barriers with high-tech surveillance features and aerial reconnaissance (Vallet 2016: 53). Advancements in surveillance were the first upgrades for border patrol stations, as global increases in cross-border traffic corresponded with augmented pressure for states to monitor and manage this movement (Broeders 2011: 21). Primarily involved in the development of aerospace and defence technologies, companies such as Raytheon, Northrop Grumman, Lockheed Martin, Boeing and Ericsson now are repositioning their products towards protecting national frontiers against more abstruse threats – as opposed to identifiable enemy combatants. Aside from the major players, there are also many new market entrants attempting to capitalise on the global multi-billion dollar border security market, a few of which have already begun testing their products for further iteration. Since the US continually spends more on border control than any other country, most implementation trials take place along their borders, as discussed below.

Radars transmit radio waves in order to determine an object's position and velocity, while various types of sensors may use light or heat to detect objects. In the town of Roma, Texas along the US-Mexico border, patrol agents use Tethered Aerostat Radar System (TARS) blimps[4] watch towers, drones and helicopters with powerful infrared sensors that were

[4] Which are similar to Joint Land Attack Cruise Missile Defence Elevated Netted Sensor System (JLENS) blimps, which are an armed version of the blimp (Raytheon nd).

repurposed from the Department of Defence's missions in Afghanistan (Long & Barrios nd); this machinery was previously used to track and monitor the Taliban (Nixon 2017). TARS use two tethered, helium-filled airships, called aerostats, that float around 10 000 feet (around 3 000 meters) in the air. The blimp can be as large as the length of a football field, and can scan a territory the size of Texas (Raytheon nd), clearly extending far beyond the immediate radius of the borderline itself. While the blimps have been successful in detecting impending aircraft attempting to airdrop drugs across the border, they are also capable of detecting vehicles and other moving objects for miles within Mexican territory. This brings into question the legality of whether or not the US should be able to peer over into the lives of foreign citizens, placing an unconsensual hovering eye over communities that may not even be alongside the border.

Quanergy, a Silicon Valley startup, is testing the installation of its LiDAR sensors along the US-Mexico border. LiDAR stands for Light Detection and Ranging, which is a remote sensing method that pulsates light to measure distance and graph shape, and it is the same laser-based processing that gives operable vision to self-driving cars (National Ocean Service 2018). The laser can detect objects and humans in a variety of weather conditions, during the day or night, providing real-time three-dimensional object classification and tracking (Quanergy Systems 2018). LiDAR can use 'topographic, near-infrared lasers' to map the land, and 'bathymetric water-penetrating green lasers' to measure seafloor and riverbed elevation levels (Quanergy Systems nd). These sensors allow for machines to 'see' their environment, even below water. This could be used in search and rescue missions to save the lives of refugees who have fallen overboard, but instead it is being used to facilitate their capture.

Radars with 360 degree surveillance, light, heat and soundwave sensors are built into military-grade drones, drive-through beams, and individual body scanners. Thermal fencing is also a solution offered by many defence companies, using heat-detection as a means of monitoring perimeters. As described by Josef Gaspar, Chief Financial Officer of Elbit, an Israeli defence contractor, '[t]he electronic solution has far more advantages than any physical [barrier]. It detects early, long range, and the information is gathered from multiple sensors' (Reed 2016). The problem arises when these radars and sensors are being used to locate and track migrants, which leads to overcrowded detention facilities.

While sensors collect data concerning object location and classification, other thermal imaging and high resolution cameras are conjunctively operating in order to further detect and identify moving people on the ground. Unmanned aerial vehicles (UAVs or drones) combine cameras, lasers and sensors, and although they are increasingly used they are relatively cost-inefficient. US Customs and Border Protection completed 635 drone missions in the 2017 fiscal year, totaling over 5 625 hours of flight (Office of Inspector General 2018). The US flies nine drones along the southern border, but they have only assisted in 0,5 per cent of apprehensions at a cost of $32 000 per arrest (Bier & Feeney 2018). This cost does not account for the value of privacy, which is fully neglected since no warrants are needed for border patrol-related UAV use. However, as argued by Koslowski and Schulzke (2018), drone surveillance also creates new accountability mechanisms, and supervision of patrol officers may also lead to more calculated and cautious behaviour by police and guards.

Elbit,[5] an Israeli defence contractor, has created a Groundeye system that can establish 'virtual safe zones' which establish an invisible fence around the perimeter of an area via mast-mounted tripods that notify operators when a person or vehicle crosses into the 'safe zone' area. Groundeye is able to 'zoom into multiple target areas of interest, while offering easy maneuverability between different areas according to operational requirements, and facilitating continuous reception of data and video coverage as well as high-quality image resolution in all areas of surveillance', which applies to both sides of the border (Elbit Systems 2016). Similarly, Northrop Grumman positions itself within the border patrol market by selling intelligent AlertVideo surveillance and geospatial imaging systems, which the US Marine Corps have used to improve decision-making capabilities for military operations along coastal zones (Fleming et al 2009: 213). The company describes these systems as being able to 'extract valuable behaviour and event information from existing surveillance systems and provides instantaneous visual and audible alerts' to the border patrol officers on watch (Northrop Grumman 2004). These integrated IoT communications networks are more quickly collecting information from previously-installed technologies, categorising that data and sending it back to government agencies. If migrants are considered to be a threat, then determining what is 'valuable' information to extract from surveillance footage can be interpreted varyingly, and whatever information is collected is systematically done without prior consent of the individuals.

Graduates of MIT's Media Laboratory founded Zebra Imaging in 1996, which first sold its holographic printers to the US military for deployment strategising in Iraq. However, now three of these million dollar printing machines are stationed at border crossing points in San Diego, Tucson and El Paso. To create these holographic maps, a drone first captures an aerial photograph of the border zone, and then uses the 360 degree view that the machine creates to construct a three-dimensional display of the landscape on the ground, better allowing for realistic targeting when deploying missions. Rick Black, director of government relations for the company, stated that 'the government brings in multiple agencies in emergencies that may not all operate in an area – like with the large Central American migrant issue', referring to the flow of migrants from Guatemala, Honduras and El Salvador that have been travelling north into Mexico and the United States (Hoffman 2016). 'Now [border patrol] can all understand where they are', Black explained, 'There's nothing else out there like this printer in the world' (Hoffman 2016). The EU Travel Information and Authorisation System (2017) credits holographic visualisation as an important tool for its security operations: 'The images

[5] Elbit Systems is also a prominent company in the military defense technologies and services, with a presence in Europe, the Americas and Asia. Elbit describes itself as a company that sells 'digital soldiers' for a nation's combat needs, and has been granted multi-million dollar contracts to secure national borders. Elbit was responsible for building the 'smart' wall along the entirety of Israel's border with Egypt, which is both above and below ground. The wall was completed in 2013, and while there were around 12,00 migrants crossing this border in 2010, only about 12 crossed in 2016 (Elbit Systems, n. d. b; Elbit Systems, n. d. a; Reed, 2016).

create better battle-space awareness in order to give border security a better vantage point when trying to prevent or defend themselves against danger. Should danger actually strike, the holographs can be used to evacuate areas and help in recovery efforts.' In this instance, the discourse seemingly is directed towards combating terrorist activity along EU borders, but it is not specified. Rather than using this technology to intercept migration flows and capture refugees, states could better protect migrants in the event of extreme danger. Refugee camps are typically overcrowded with confined streets and layered cohabitation, and 3D models of the sites could help to better plan and execute emergency evacuation plans in the event of terrorist activity or a natural disaster. There is no evidence that this technology is being used to protect all lives, only American and European lives.

Member states of the EU and the regional body itself have for over a decade been logging, storing and monitoring migration databases concerning the inflow and outflow of passengers (Broeders 2007: 71). All the information collected is then analysed through centralised intelligence stations, where the data must be processed, stored and disseminated in a useful way. With such amassed amounts of data, algorithms are being used to analyse the content more quickly – an example being IDEMIA's Morpho Video Investigator, which automatically hones in on faces, bodies, motion and licence plates (IDEMIA nd). Algorithms are simultaneously sorting through video footage while also referencing volumes of raw data in order to record and classify elements deemed to be 'of interest' to law enforcement and the intelligence community. The greatest risk lies in misappropriated uses of what the government deems to be 'of interest'. The EU Travel Information and Authorisation System (2017) determines that any border technology implementation will work towards fulfilling the 'same goal of keeping citizens as safe as possible from terrorism and illegal entry,' thereby posing refugees as a threat and equating a person fleeing conflict with a terrorist. IDEMIA (nd) is already in use by governments within Europe, Latin America, the US, Asia and the Pacific, but not all countries have policies stipulating how the algorithmic conclusions of the system can be ethically used. There have already been instances when government-collected data is kept longer than presumed legal, which was the case when 35 000 images of citizens' body scans from TSA airport security leaked in 2010, even though US policy stated that all images are 'automatically deleted from the system after it is cleared by the remotely located security officer' (Johnson 2010). Global inconsistencies in how these algorithms are translated into government policy and an overall misunderstanding of how said policy is implemented leave ample room for mistakes without consequence.

3.2 Technology of the future, happening now

Collecting biometric data, via fingerprinting, has been a means of border-crossing identification for travellers since the mid-1990s when the United States created IDENT, the Automated Biometric Identification System (Gemalto nd). Worldwide, it has become more commonplace that fingerprints are taken at international transit points, and this personally identifying stamp can be used to determine an individual's eligibility for entering or exiting a country. Biometric data, as defined by the European Commission's Department of Migration and Home Affairs, is 'data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images or dactyloscopic data' (European Commision nd). Biometric data collection has since evolved to include the reading of irises, facial bone structure, the distance between one's eyes, nose and mouth, and so forth. The IT systems incorporated into the machinery that have been mentioned thus far in this report often store biometric data. All individuals participating in the US-VISIT programme – including persons with visas and green cards – must submit digital photographs and fingerprints providing biometric data to the federal, state and local governments (Mason nd). To date, biometric data and other personal information has been collected from over 200 million people who have entered, attempted to enter, or exited the United States (Gemalto nd). While the US plans to install more advanced biometric-based systems in all major airports within four years (TSA 2018), biometric data is also a required component of applications to enter Schengen states, which have collectively issued 14,6 million visas for short stays in 2017 alone (Schengen Visa Info 2018). On 8 April 2019 Singapore's Immigration and Checkpoints Authority (ICA) (2019) began testing iris scanning as a means of identification that replaces the need to show a passport. The iris scanner logs the unique patterns within the coloured circle of the eye, and capturing a person's biometric stamp only requires a person to look at the camera for one to seven seconds (ICA 2019). ICA states that the government's back-end database will determine if the traveller holds a valid passport and necessary visa in order to grant access. While iris recognition improves identification accuracy, reduces the likelihood of forgery and enhances efficiency at transit points, the tech companies that are incorrectly describing this technology as 'non-invasive' considering data could be collected surreptitiously, without individuals' knowledge (EFF nd). Additionally, if this information is hacked or leaked, then the responsibility lies with the third party vendor where the databases are stored and citizens may not even know that their information is being housed within these companies. If the result of non-compliance is the denial of access to the country, then ultimately the traveller is left with no choice as to whether or not they consent to have their irises read.

Anduril's Virtual Reality (VR) devices, backed by artificial intelligence, are currently undergoing testing by US Customs and Border Protection along the Texas border (Levy 2018). These devices, however, are not simulation based; they are being fed live information that is picked up by radars and laser-enhanced cameras that have been installed at high altitudes for a grander purview. The surveillance equipment can detect motion at approximately a three kilometre radius, and then locks on a target to determine its classification – 88 per cent likelihood of it being a person; 93 per cent likelihood of it being a plant; 76 per cent likelihood of it being an animal, for example (Anduril nd). The software that allows for communication between these systems is called Lattice, which synthesises data from potentially thousands of sensors and translates that into images on a Samsung Gear VR headset. On screen, the categorisations are highlighted making it easier for the human eye to determine where a target is moving or if an object in motion is worth noticing. Although still undergoing tests for further development, Lattice's experimental trial in Texas already assisted customs agents in detaining 55 'unauthorised border crossers' (Wodinsky 2018). According to their current business model, the data Lattice collects will belong to whatever agency has purchased a leased contract for the technology.

Based on the direction and rapid frequency of technological updates, it is likely that facial recognition technology will start specifying classifications of people that are seen through the VR goggles – by sex, gender, age, nationality, criminal status, and whatever other information the government may wish to reference against volumes of big data. China, for example, a country known for hyper-surveillance, has been using facial recognition technology to track and control the Uighurs (Uyghurs), a Muslim minority group. This has been called the first known example of a government utilising artificial intelligence for racial profiling, leading towards a 'new era of automated racism' (Mozur 2019). With this kind of virtual reality software serving as a gatekeeper for our borders, the potential for ethnically-motivated segregation is a grave concern.

Artificial intelligence is the science of building technology that can mimic human intelligence by instilling 'logic' into an algorithm or machine. Machine learning is a subset of artificial intelligence, and is based on a machine's ability to make choices based on algorithms that feed neural networks and decision-making models, which are continually adapting to new information in order to self-improve. The ability for a machine to change algorithms as it learns more information is what differentiates machine learning from the broader category of artificial intelligence, and both of these advancements are being quickly adopted by law enforcement. In 2017 the West Midlands Police Department in the UK announced the development of a system called NAS (National Analytics Solution), which is a predictive model that can 'guess' the likelihood of someone committing a crime (Portilho 2019). The programme utilises machine learning as a means of combining related data sets – from other partner agencies as well as the Department of Education, the Department for Communities and Local Government, the Department for Work and Pensions and the National Health Service – to determine statistical probabilities prior to a person having committed the offence (West Midlands Police nd: 22). Therefore, neural networks will process data sets regarding people's employment status, education levels, community involvement and health conditions (potentially mental and physical) in order to predict whether or not they are a threat to society. This kind of preemptive judgment has massive human rights ramifications, targeting individuals prior to an actual offence having been committed – nullifying the entire conceptual understanding of a right to a fair trial. The Alan Turing Institute's Data Ethics Group (2017: 5) denounced the use of NAS, stating that '[w]e are generally concerned that the development of ethical principles in the NAS is not at a sufficiently advanced stage to permit them to keep abreast of the proposed uses of technology and data analytics for a new and wider law enforcement mission'. Border patrol is considered a branch within law enforcement, although thus far there is no evidence of patrol agents utilising this technology.

While machine learning is becoming pivotal in the field of medicine for more accurately diagnosing disease, and businesses are becoming more heavily reliant on its ability to sort through large amounts of data and detect patterns, a major underlying flaw in using machine learning for profiling is that the datasets may be biased or even doctored (Papernot et al 2017: 13). It is possible to reverse engineer algorithms in order to produce a desired output, which is why the true intelligence of the machine is influenced by the prejudice or intentions of its creator. Regardless, the artificially intelligent machines at our borders lack the contextual knowledge of what human rights are, and have yet to be programmed with valuable insights on important bigger picture factors, such as the causes of global migration waves, personal concerns of privacy infringement, the stark effects machine decisions can have on an individual's life, to name just a few.

While humans are trying to teach artificial intelligence to machines, researchers are trying to recreate the marvels of nature by studying the flight patterns of birds and insects. Micro Aerial Vehicles (MAVs) are small robotic drones with cameras and built-in microphones and can be as tiny as a few centimetres (US Air Force Recruiting 2015). MAVs can work individually or in a swarm to infiltrate a sensitive areas, where larger drones would be too bulky or noticeable, and transmit information back to a control centre. Considering that UAV surveillance has become more commonplace, it is not far-fetched for border patrol to further their surveillance efforts by employing MAVs. The MAVLab (nd) at the Delft University of Technology in The Netherlands specialises in micro and nano-air vehicle research, as does Harvard's Microrobotics Lab, and departments within MIT.

Considering that this type of surveillance is designed to be incognito, the infringements upon privacy rights are flagrant. A goal of MAV aeronautical engineering is for the device to be capable of accurately landing on the human skin, and potentially collecting DNA samples or detecting chemical radiation (Office of Communications 2012). Policy relating to the use of these machines at transit points needs to be discussed at greater lengths with more transparency as to their capabilities and applications, allowing for an interdisciplinary approach to important regulation for technology that has unprecedented consequences.

3.3 Human rights implications

The effects of utilising fourth revolution technologies will continue to be a morally-charged issue, and voters without a detailed understanding on matters of privacy versus security will remain in a haze of doubt. At present, advancing technologies are contributing to an already dehumanising and under-resourced flood of immigration casework. Steven Levy, a tech correspondent for WIRED, addressed the human rights concerns that arise when painstakingly omniscient technology begins to infiltrate sensitive situations:

> Families are not part of the Anduril [executives'] thought processes. They're fulfilling what the government wants done and they aren't getting involved in the politics. But what we are learning is that technology is politics. They consider themselves as patriots doing this for the government, but you can't do this without dealing with the implications of your technology (CNBC 2018).

Under the Trump administration's 'zero tolerance' immigration policy, close to 3 000 children were forcibly separated from their parents and placed in shelters – some with extremely poor conditions – or foster care (Office of Inspector General 2019:1).

Reviewing the equipment used by the border patrol agents, it is clear that militarising the border means far more than just deploying troops manned with heavy artillery weaponry. The same technology being used to hunt high-profile enemies of the state and internationally infamous terrorists is being used to peer over state lines and detect the movement of migrants in neighbouring countries. Operating under the guise of national security is an ethos-driven argument for patriotism, yet the implications of surveillance with piercing accuracy include dangerous human rights violations.

As explained by Lyon (2007: 7), if the objective of surveillance is social sorting, then systematising classifications of people merely precedes unequal treatment. In the case of migration, this translates to either granting or rejecting access to state territory, visa privileges or asylum status. Digitising the border via artificial intelligence, integrated IoT communications networks, and biometric data collection can lead to formulaically differentiating between which people governments consider to be more valuable. Artificial intelligence is already sorting cargo in the EU, as explained by Sven Suurraid, head of the customs department for the Estonia Tax and Customs Board: 'It's nice to have very modern railway X-rays but the analysation of the images must develop to the next level, not made by humans. Our future is in pairing machine learning and artificial intelligence to check these pictures' (Lewington 2018). Will humans be processed in the same way?

When machine-learning outputs include solutions based on one-dimensional algorithms, the risk lies in an inability to programme the essence of morality into a technological system, leaving all other dimensions related to human rights behind. Bowling and Sheptycki (2015: 151) argue that law enforcement and all of its peripheral branches will increasingly rely on technology, but officers must remember that 'a device is more than just a technological tool and should be seen as an important component in the process of transnational policing and in the deployment of specific rationalities in the governance of security'. As suggested, technology is a mere component to the larger picture, as there are many other sensitive factors at play when dealing with migrants, refugees and asylum seekers. A state's border security strategy should incorporate cooperative neighbourly relations in order to achieve the common goal of filtering out smugglers and terrorists, all the while stimulating business, cross-cultural value sharing, and ensuring that all people have the right to be treated with dignity.

As in the case of all new technologies, its application is more important than the technological development itself. There are infinite examples of how technology has been used to help humankind, but it has only ever been accomplished with a person who values humanity driving the achievement.

4 The impact of digital walls and data-driven barriers on vulnerable groups

In the past, humans were responsible for managing tasks and risk along the border, meaning a conscious mind would make the final decisions. However, these tasks are now increasingly being carried out by machines, implying an algorithm may decide the future of a human's fate.

This part of the article examines the impact of border digitisation on individuals, particularly focusing on the discriminating effects pertaining to vulnerable individuals or groups. It explains how a machine can hold biases and the extent to which algorithmic discrimination can be applied at the border. The interactions between facial recognition systems and vulnerable groups, including dark-skinned women, are the basis for this section, which explains how machines can impose discrimination and further disadvantage the most vulnerable groups in society.

A machine itself is not discriminatory, but machine-learning algorithms can be shaped to be so. Facial recognition is performed by automated facial analysis algorithms that are trained with datasets, which contain thousands of pictures of faces. By training the algorithm with those pictures it can learn to recognise and classify faces. A comparative study carried out by Buolamwini and Gebru (2018: 77-79) showed that some of the widely-used datasets are composed of samples where more than two-thirds of the images are light-skinned faces. Therefore, the algorithms trained with these skewed datasets will be much more precise in recognising light-skinned people over dark-skinned people. The study by Buolawinis and Gebrus not only reveals that the trained algorithms have problems correctly identifying dark-skinned people, but they also have a gender bias. Many women were wrongly detected as male or not recognised as human faces at all. Females were underrepresented in the dataset, which resulted in an average error rate for dark-skinned women as 34,7 per cent, whereby light-skinned males were misclassified by only 0,8 per cent (Buolamwini & Gebru 2018: 77-82).

These kinds of skewed datasets are not only used for facial recognition systems by tech companies, such as Apple installing facial recognition into their products, but also by the police to enforce the law. Consequently, public authorities make decisions based on these flawed systems. For instance, in some US states law enforcement uses a facial recognition system called Rekognition provided by Amazon (Cagle & Ozer 2018). Shortly after the publication of the Buolawinis and Gebrus study, the American Civil Liberties Union (ACLU) tested Amazon's software. The ACLU results were shockingly similar to those of the Buolawinis and Gebrus study, which tested facial recognition systems from other providers. ACLU's test proves that Rekognition was trained with a dataset predominantly made up of pictures of light-skinned people (Snow 2018).

Test results such as these triggered Amazon's shareholders to call for a bar on selling facial recognition systems to law enforcement. The shareholders were particularly concerned about civil and human rights violations (McFarland 2018). Wood (2018) points out in Amazon's official AWS Machine Learning Blog that Rekognition can be used to fight crimes such as human trafficking or child exploitation and that any unlawful use or harmful act towards someone with the software is prohibited. Facial recognition systems might have some positive uses and make several areas of work more efficient. However, even in lawful use and properly exercised by professionals, algorithms can be biased and, therefore, discriminatory.

Concerns about facial recognition systems and their impact on civil and human rights have already proven to be valid. The danger of such systems stems, on the one hand, from the issue of racial and gender bias. On the other hand, it lies in how this biometrical technology is used in practice. It can lead to unfair practices and discrimination due to biased profiling. Unfortunately, technologies have evolved so fast that legal regulations have not yet caught up, which is particularly important to observe in the US.

In the context of border management, facial recognition systems are most often used to conduct profiling. Profiling is a way of categorising individuals on the grounds of changeable or unchangeable characteristics. The collected data is converted into profiles and stored for a certain amount of time (European Union Agency for Fundamental Rights 2018a: 15-16). It is important to note that profiling, exercised either by humans or systems with an underlying algorithm, is always – consciously or unconsciously – biased. Algorithmic systems are biased because of previous learning experiences or from the database that trained the algorithm. Those biases influence the profiling assessment as well as the decision making (European Union Agency for Fundamental Rights 2018a: 18). Thus, there is a high risk for discrimination. In other words, profiling is unlawful if an individual or a group of people would be treated less favourably than another person or group in a comparable situation as a result of targeting due to subjective justification (Council Directive 2000/ 43/EU, Article 2, 2000). In addition, using a biased algorithm in a facial recognition system could lead to structural discrimination.

However, facial recognition systems are becoming standardised for profiling at most border checkpoints. There are two main reasons for conducting profiling in border management: first, to identify individuals. This is important in order to find out whether the subject is already known or not, and if there is already a history with that individual. Second, profiling is used to predict behaviour and to make decisions concerning the profile due to these predictions. This is especially important for security and law enforcement reasons, and even of greater importance if the subject is not yet known in the system. Such a presumption could be the likelihood of the person remaining in a country after their authorised stay has finished. With the presumptions regarding the subject generated from the system, border management has an additional tool to decide what kind of policing (proactive or reactive) is adequate for the situation.

In the EU Schengen zone, facial recognition is being tested for entry/exit situations. By collecting biometric data, policy makers hope to maximise security by minimising the falsification of travel documents and illegal stays. Augustin Diaz de Mera Garcia Consuerga (2017) from the European Parliament points out that security- and preventive-driven policing became more prominent after the increased mixed migration flows towards Europe in 2015 and several terrorist attacks – such as the 2016 Berlin attack when the police uncovered that one of the assailants had used 15 different identities.

Amassing vast amounts of personal data and conducting profiling are methods being more frequently used in combination with algorithms to create coded solutions for automated decision making (ADM). Algorithms with ADM have been a fixed part of our lives for a while now. One of the most common examples is the spam filter in every inbox (European Union Agency for Fundamental Rights 2018b). Sometimes an e-mail is moved to the spam folder by the algorithm, despite it being an e-mail that typically would not be regarded as 'junk mail'. The same thing happens when using ADM at border crossing points, especially when the algorithm contains racial and gender biases. A refugee woman could be wrongly detected as someone who has already applied for asylum and would therefore be rejected. ADM is applied frequently and the reasons why it is used could turn out to be more dangerous than anticipated. This danger provides reason for legal regulation that must be kept up-to-date with technological developments.

The EU law is more developed than the US law regarding the regulation of profiling and ADM. Regulation (EU) 2018/1725 applies to personal data proceedings directly executed by an EU governing body, organisation or agency. This regulation allows the EU to collect and process intimate personal data if an EU body needs the data to fulfil its mandate. This usually applies in the context of security such as border management. In practice, this means that Frontex is only allowed to use ADM under certain circumstances. Therefore, in most cases Frontex is obliged to use profiling as an additional tool to gather information but not to make decisions solely based on this technology. This minimises the risk of vulnerable parties falling victim to a biased or incorrect algorithm.

In addition to Regulation (EU) 2018/1725, the EU also regulates profiling and ADM under the General Data Protection Regulation (GDPR). This is important because of the limitation on data mining and surveillance performed by private companies. The GDPR prevents the gathering of personal data in another context in addition to prohibiting the sale of that information to law enforcement. Under article 22 §1, GDPR (Regulation (EU) 2016/679, article 22) profiling is only accepted under the condition that the decision cannot solely be based on ADM and it shall not affect the data subject in a significant way. Even though article 22 §2 allows profiling under very specific circumstances, article 22 §3 restricts this profiling. It does so by referring to article 9 §1 GDPR, which regulates processing of special categories of personal data (Regulation (EU) 2016/679, article 9). These include, among other personal data, genetic data and biometric data, which are extremely sensitive because they remain unchanged for a very long period of time (Deutsches Referenzzentrum für Ethik in den Biowissenschaften 2019).

In situations such as border management, profiling can have a very serious impact on minorities or vulnerable groups such as dark-skinned women. Nonetheless, profiling is widely used in border management and in some countries even in combination with ADM (Osborne Clarke 2018). Facial recognition systems are not the only AI systems with algorithmic discrimination. In recent years more systems have developed similar problems. However, as a result of these other systems being largely used among different sectors, facial recognition systems have come under more prominent scrutiny than others. Nonetheless, the legal framework still has to keep up with the fast evolvement of new technologies, which is discussed in more detail in the next part.

5 Balancing security and human rights: Analysing the shifting policy and legal frameworks on digital walls and border surveillance

As discussed above, means of surveillance have greatly transformed since the beginning of the twenty-first century. What started as traditional, manual mechanisms rapidly shifted towards new, automated technologies,[6] which have proven to be cheaper, faster and able to deliver thousands of terabytes of information and knowledge in a single chip. This part first focuses on the shift in policy making that has taken place in response to the expansion of surveillance and biometric data collection in law enforcement, using the US and Europe as case studies. It addresses the risks and consequences of constant border surveillance and concludes with an analysis of the present legal framework and attempts to balance security and fundamental rights.

After the 9/11 attacks people's perceptions of privacy and security changed radically, not only in the US but worldwide. As a global political narrative began to focus on border control, civilian attention also began narrowing in that direction. Emergency driven policies transformed into organised intelligence, in which constant mass surveillance became necessary for law enforcement and national security. The increased number of surveillance mechanisms and high-profile biometric devices pending patent registration reflects this change in policy and mindset. Between 1970 and 1995 the US Patent Office granted fewer than ten patents involving facial recognition systems. From 1995 to 2000 it issued 20 such patents. Between 2001 and 2011 the number leapt to 633 (Donohue 2012: 410).

Emergency-driven policies, which tried to tackle problems once they materialised, became obsolete within policy making as governments shifted towards a risk-management approach, which focused on prevention as the main way to avoid terrorism, (non)-organised criminality and irregular migration.

In practice, however, the risk management approach often is not proportional to the limitations of rights it brings with it, consequently becoming too invasive (Degli Spotzi 2018: 79). With massive surveillance operations, there is a tendency to move from contextualised surveillance to a generalised surveillance through the collection of purely preventive information, carrying with it the respective violations of the fundamental right to privacy.[7] From a human rights law perspective, this approach should incorporate a proportionality test, as it should analyse risks in accordance with overall risk tolerance and decide whether or not the limitation of civil liberties is warranted. Since border surveillance suggests a threat to privacy by enabling widespread surveillance and massive personal information storage in databases (Nissenbaum 2010), the privacy-security trade-offs must be carefully assessed. The so-called risk-management approach has inevitably taken us to profiling and uninterrupted data storage as common practices. Border agents have used profiling as a modern tool for identifying and categorising people in order to detect threats within the stream of border traffic through data mining, as explained in the previous part.

Establishing what a legitimate limitation of rights entails can be a daunting task. While surveillance for illegitimate reasons violates privacy, surveillance for legitimate purposes can also do so if the associated privacy harms are not proportional to the ultimate purpose (Latonero 2018: 149-161).

[6] Automated technologies are those operating by automatic means, reducing the human intervention as an operator to a minimum.

[7] Art 12 UDHR; art 8 ECHR; art 7 EU Charter of Fundamental Rights (ECFR).

In the current context of high migration flows, both border agents and governments have been accused of profiling (Panneta 2019) and of data retention[8] as an abuse of privacy (Massé 2016). As explained in this article, efforts to increase biometrical identification systems are spreading fast around the world. Within biometric identification, there are two types that have been widely used (Donohue 2010: 414-415), namely, immediate biometric identification (IBI) and remote biometric identification (RBI). IBI is focused on a single individual, with a close-up, and it is used in particular for detention purposes in a government-owned area. RBI, on the other hand, gives the government the ability to determine the identity of multiple people, both in public spaces and at a far distance (Donohue 2010: 414-415). As part of the risk management approach, the federal government in the US has increasingly invested in RBI technologies to supplement its IBI capabilities (Donohue 2010: 414-415).

The legal nature of these two types of biometric identification is different. Whereas IBI involves notice and consent and is limited in its occurrence, RBI does not require notice or consent, as it is done in a continuous manner (Donohue 2010: 414-415). This distinction is especially important in the context of border management, since millions of people are crossing borders daily. Surprisingly – or perhaps not – all this personal information is stored in servers that are not accessible to the public, raising concerns about data privacy and potential misuse. The same concerns apply to facial recognition technology (FRT), as this allows governments to observe and retain data in public spaces. China started a national surveillance system comprising 200 million cameras, with plans to have 300 million cameras in place by 2020 (Mozur 2018). China is also using its mass surveillance capabilities to create a system of 'social points'; the government is tracking people's habits, like online shopping behaviour or smoking in public, to grant and detract from civic rights and opportunities (McDonald 2018).

In response to all these privacy concerns, each government's script is often the same: National intelligence agencies promise to minimise terrorism and crime with the retention of our personal data. States often defend this by saying that it is not an intrusion into our private sphere. However, evidence such as the Snowden revelations has shown that there is a permanent state of surveillance by states of people both at borders and within them (Greenwald 2013).

As far as mass data retention is concerned, Frank La Rue, the former UN Special Rapporteur on Freedom of Expression, acknowledged:

> National data retention laws are invasive and costly, and threaten the rights to privacy and free expression … [M]andatory data retention laws greatly increase the scope of state surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to theft, fraud and accidental disclosure (A/HRC/23/40).

[8] Art 5(e) GDPR: [Data should be stored for] 'no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'.

This shows not only how we are subject to mass surveillance, but also the risks of such mass surveillance. The legislative framework in place with regard to data retention contains many shortcomings. These shortcomings increase the risk of human rights violations, as they allow for the use of data to limit access to certain territories, curtail freedom of expression and hamper personal data sovereignty due to the creation of long-lasting personal files. These not only present an immediate risk, but raise concerns for greater risks in the future, depending on the judgment of those in power.

There are no worldwide legal provisions that regulate and protect the processing and storage of biometric data. Instead, the overall trend is to include the collection and use of biometric data within the framework of personal data protection and domestic privacy laws (Council of Europe 2018). The intangible nature of data poses a complicated dichotomy. In practice, data flows freely across geographic borders, but the territorial scope of data protection laws is restricted. While border digitisation undeniably affects privacy and data protection, practice shows that the lack of territoriality of the internet also poses grave concerns for the right to privacy. According to Justice Abella from the Supreme Court of Canada, '[t]he internet has no borders – its natural habitat is global' (*Google v Equustek* 2007). Collected data from government surveillance similarly is borderless.

In the US only a handful of states currently regulate biometrics within their legal frameworks,[9] and there is no framework regulating patents whatsoever. Unlike in Europe, privacy is not a fundamental right in the US, where it is often balanced against the Fourth Amendment. The 1974 US Privacy Act regulates how the federal government holds personal data and stores it. However, it is important to know that there currently is no single principal data protection legislation in the US. Furthermore, at the jurisdictional level, the courts use the reasonable expectations of privacy principle, which is an element of privacy law that determines in which places and during which activities a person has a legal right to privacy. Whereas this principle is used to protect against undue interference in private life, it makes the right to privacy dependent on the situation and context, giving the impression that fundamental rights are dependent on a person's circumstances.

In Europe, on the other hand, the GDPR entered into force in May 2018 and represents the culmination of Europe's efforts to be at the forefront of data protection. The scope of application of this law is limited to private organisations, companies and individuals processing personal data of EU citizens or foreigners based in the EU. Described as a very sophisticated law (Guido Raimondi 2018), the GDPR introduced a new sanctionatory structure, in which non-compliance can lead to fines of up to €20 million or 4 per cent of a company's annual worldwide turnover (GDPR 2018, art 83.5). This law applies to subjects 'whatever their nationality or place of residence' (GDPR 2018, recital 14) within the EU. It is of utmost importance since it regulates the information that could fall into the hands of private companies within the context of border-crossing. In addition, Directive (EU) 2016/680 is used for applying the GDPR when law

[9] Illinois, Texas and Washington, for example, have passed biometric privacy laws subsequently since 2008.

enforcement is involved. It regulates the processing of personal data of natural persons by competent authorities, for the purposes of the prevention, investigation, detection or prosecution of criminal offences (GDPR 2018, recital 19).

The GDPR also provides a clearer definition of consent, which changed from merely 'freely given' to 'freely given, specific, informed and unambiguous'. This change was most likely prompted by the fact that privately-run companies, and sometimes governments, often hide behind the mask of consent to renounce any responsibility, as Facebook did in 2018 (*Federation of German Consumer Organisations (VZBV) v Facebook* (2018)).

In order for consent to be valid, data subjects must be given a genuine and free choice. This essentially eliminates forced consent within the borders of the EU. In other words, when two parties sign a contract and the one party has no way of declining consent without suffering a consequence, consent is fundamentally biased. This applies even more so to situations in which consent is not even explicitly given, such as in the context of border surveillance. As a consequence, the idea of consent as we know it today has led some academics to refer to consent as a myth (Degli Spotzi 2018: 177).

When the EU (as an institution) is collecting data, the regulation applicable is Regulation (EU) 2018/1725, which is fully in line with the GDPR. This regulation lays out the data protection obligations for EU institutions and bodies as they process personal data and develop new policies. It is enforced as soon as EU agencies come in contact with data. However, its scope is wider because of the protective mandate of such institutions. For example, it would regulate how Frontex deals with refugees' personal data.

In Europe article 8 of the European Convention for the Protection of Human Rights and Freedoms (ECHR) on the right to respect for private and family life is central to the privacy-security trade-off debate. The European Court of Human Rights (European Court) has balanced article 8 with conflicting interests such as private property and national security. If a state were to limit article 8, this interference would have to be 'necessary in a democratic society', meaning that there must be a 'reasonable' 'pressing social need' (Council of Europe 2019) for such intrusion in the private sphere.

This privacy-security conflict is addressed in cases such as *Klass & Others v Germany*. In this case the Court held that there had been no violation of article 8, finding that the German legislature could draft legislation empowering the authorities to monitor people's correspondence and telephone communications without having to inform them. This case was made on the grounds of national security and public interest. In *Malone v United Kingdom*, however, the Court held that there had been a violation of article 8 when the government tapped communications, and constantly monitored them without reasonable clarity or scope.

Similarly, on 6 October 2015 the European Court of Justice (ECJ) issued its judgment in the case of *Schrems v Data Protection Commissioner,* declaring the European Commission's Decision 2000/520/EC invalid, which allowed transfers of personal data from the EU to the US. While the

Schrems judgment only directly concerns data transfers from the EU to the US, its ramifications may indirectly affect cross-border data transfers more generally. In the same way, the ECJ issued Opinion 1/15 on 26 July 2017, and as interpreted in the *Schrems* judgment, the transfer of data to a third country became possible only if such country ensures an adequate level of protection.

In the *US v Jones* case (2012) the US Supreme Court established that monitoring a car through the use of GPS constitutes a violation of the Fourth Amendment, the principle that protects people against unreasonable searches. The Court ruled that the GPS monitoring was disproportionate in time and space and it was a trespass of Jones's personal effects. Similarly, in *US v Maynard* (2010) the Court established that attaching a GPS to a person's vehicle without a warrant constitutes a violation of the Fourth Amendment. The Court stated that 'a person who knows all of another's travels can deduce whether he is a weekly church goer, an unfaithful husband … and not just one such fact about a person but all such facts'.

Furthermore, while border surveillance can potentially be a threat to civil liberties, it is particularly apparent that those who have the power to control surveillance are the ones who can abuse it of their own volition. Reports claim that in 2016 Donald Trump's personal lawyer allegedly met with a KGB operative in Prague, despite the fact that his passport holds no proof of entry to the Czech Republic (Stone and Gordon 2018).· If accurate, this case may show how border surveillance, rather than merely following traces based on stamps within passports, can function as a means of transparency. Technology allows tracking to be done independently of there being evidence of a border having been crossed or not, which may result in holding elected officials accountable. Not surprisingly, border technology and surveillance is a controversial political issue, and the next part examines this political dimension in more detail.

6 Populism and digital walls: Analysing the political challenges to implementing human rights-friendly border technologies

Political will heavily influences the likelihood of border technology complying with human rights obligations, and thus determines whether smart borders amount to smart solutions. Therefore, this part examines the political playing field, focusing on the influence of right-wing populist parties. The emphasis is on the EU, but events in this region reflect the growing international support for populist leaders (Kyle and Gultchin, 2018).

Going forward the rise of populism could present a challenge to human rights protection in border technology. A central contention of this article is that the rise of the populist far-right in Europe is playing into the securitisation culture surrounding migration. The proliferation of securitisation in the EU coincides with the militarisation of its borders. It has been argued that these phenomena are inter-related as an enhanced focus on security at the border can justify the use of militaristic paraphernalia. Granted, numerous factors contribute to the increased use of security technologies on the EU's external borders, including the economic interests of arms traders and the fear of terrorism since 9/11.

Nonetheless, the connection between securitisation, militarisation and right-wing populists is worthy of consideration. It must be stated from the outset that the militarisation of borders predates the rise of right-wing populism. Moreover, until recently right wing populists did not wield any direct control over the EU so they did not have a direct impact on policy relating to the EU's external border. However, the trend demands attention for a number of reasons. First, right-wing populists are gaining international traction. Second, right-wing populist rhetoric extols the benefit of strong borders; and through repeating this, they encourage a shift to the right among other political actors.

This article argues against the idea that populism is irreconcilable with technology and instead contends that populist solutions are inextricably linked to emerging technologies. To further elaborate on the connection between rising right-wing populism in Europe and border technologies, this part first discusses a definition of right-wing populism and the centrality of borders in their politics; second, it addresses the significance of social media and the influence of populist discourse across the political spectrum; and, finally, outlines the relationship between securitisation and militarisation of migration.

In Europe, borders have become a political priority due to an unanticipated surge in immigration. Conflicts in the European neighbourhood and the Middle East led to an influx of migration over the past decade, peaking in 2015 and 2016 (Johansson-Nogués 2018: 529). A 2016 Commission Communication stated that the number of migrants globally in 2016 represented the most severe refugee crisis since World War II (European Commission 2016). The sheer volume of people entering the EU and the dangerous routes taken (via boat and on foot) undeniably resulted in a humanitarian crisis (Neville, SY, Rigon, 2016: 8). This crisis led parties across the political spectrum to look for ways to respond. The European Parliamentary Committee on Civil Liberties, Justice and Home Affairs repeatedly called for the creation of legal routes into the EU (Luyten and González Díaz 2019), whereas more conservative parties called for stricter border control.

Quite apart from these two responses was the response of right-wing populists. These groups not only call for stricter immigration controls but also argue that settled immigrants are corrupting the values and culture of their respective nations. Recently, the European Commission declared the migration crisis over, and the Commissioner for Migration, Home Affairs and Citizenship noted that irregular arrivals are now lower than before the crisis (European Commission Press Release Data Base 2019). Nonetheless, populists continue to warn against rising migration (Roth 2019). A 2011 Chatham House report (Goodwin 2011: x) stressed that anti-immigration sentiment is a defining characteristic of right-wing populism:

> These parties share two core features: They fiercely oppose immigration and rising ethnic and cultural diversity, and they pursue a populist 'anti-establishment' strategy that attacks mainstream parties and is ambivalent if not hostile towards liberal representative democracy.

One reason why border control is so important to populists is that it symbolises the exercise of state sovereignty. States traditionally held the power to decide how many people could enter their territory, as well as the processes for crossing the border. However, in a globalised world, states no longer have boundless discretion. Rather, they are restricted by international obligations and commitments. These include principles of international law such as *non-refoulement* protections (OCHRa 2018) guaranteed under international humanitarian law and standards set out in international human rights treaties (OCHRb 2018). Furthermore, states in the Schengen area pledged to cooperate with others in the area regarding how to manage the external frontier of the EU. Populist parties equate this diminution in the ability of the state to make independent decisions regarding migration, as an imposition on state sovereignty.[10]

Other features of populist agendas may seem unrelated to borders and migration at first glance. However, on further inspection the connection becomes apparent. For example, an identifying characteristic of populist parties is that they claim to represent 'the people'. Advocating greater accountability and responsiveness from democratic systems would seem to be a laudable aspiration. However, the populist conception of democracy leaves no room for pluralism. They portray 'the people' as a homogenous whole; the people are not just 'demos'; they are also 'ethnos' (Pasquino 2007: 16). In their 2017 World Report, Human Rights Watch (Roth 2017) noted:

> Throughout the European continent, officials and politicians harken back to distant, even fanciful, times of perceived national ethnic purity, despite established immigrant communities in most countries that are there to stay and whose integration as productive members of society is undermined by this hostility from above.

These points go some way towards explaining why borders are a site of utmost concern for populists. In populist discourse, migration is more than a question of policy; it is a question of transcendental import. Borders take on spiritual significance, in that they represent an answer to the most essential of human questions, 'why do we suffer?':

> Populism employs a secularised version of the myth of the fall of man to explain suffering as something more palatable to the sufferer. Things have gone wrong, suffering has come into the world with the others (the immigrants, the political elite, the established media), and what we need to do now is return to the paradisiacal State that existed before the fall (Hendricks & Vestergaard 2019: 93).

While they have built their rhetoric and agenda in this vein, populist parties have relied on emerging technologies to garner support. It has even been argued that the formats of certain sites encourage more radical perspectives (Bartlett 2018). Social media sites provide an ideal platform for populist parties. Simple messages sell online and populist outlooks attract more attention online than anything in the 'watery centre ground' (Bartlett 2018). Hendricks and Vestergaard (2019: 88-89) write:

> Populism is an efficient media strategy that plays on emotions. The narrative structure of us-versus-them, with the others being villains, is efficient when it comes to mobilising anger or fear. News stories that provoke anger (ie, indignation) and fear have a much greater tendency to go viral and suck attention on social media.

[10] With that said, populist parties may be willing to support European Union cooperation if the goal is to reduce all immigration, via a method they agree with.

The fault here cannot be placed squarely on new social media platforms. Instead, these platforms just exacerbate innate human tendency to gravitate towards stories that affirm one's own world view. This tendency accounts for the success of misinformation online. As Hendricks and Vestergaard explain (2019: 80), cognitive dissonance and selection bias play an important role in this context. These methods of sharing and receiving information contribute to the polarisation of the political spectrum. Etzioni (2018: 131) explains that causes of the success of populism among traditional communities include 'fragmentation of the news, gerrymandering, self-segregation, and political polarisation'. This media landscape contributed to the growth of the populist right across Europe by reinforcing outlier perspectives.[11]

The success of right-wing populist agendas online has an impact 'in real life'. Notably, even where right-wing populists have not gained a majority, the presence of support for right-wing populists in the political arena pushes centre parties further to the right. An example of this is the German tightening of border control following Chancellor Angela Merkel's initial open response to the migration crisis (Balfour 2016: 48). It demonstrates how the influence of populist candidates changes the political arena, irrespective of whether they directly hold power or not. A 2016 European Policy Centre report (Balfour 2016: 3) argues that in the current interconnected and globalised world, the impact of domestic policy discourse extends beyond state borders. Therefore, right-wing populist groups influence EU foreign policy and border management, even though they have not enjoyed parliamentary success in all EU member states.

If one accepts that the growth of populism affects the political arena, this leads to the question of how populism will affect border policy. Right wing populism contributes to an atmosphere of securitisation which can contribute to border militarisation. This is a significant factor to take into account when discussing border technologies, because where technologies are rolled out as a part of border militarisation rather than as a part of a project with humanitarian intentions, this affects the priority given to human rights.

An atmosphere of securitisation has crept over Europe. In this context, contemporary politics often presents a dichotomy between security and human rights. For example, as was discussed in the previous part, increasing data surveillance is justified by the ends of security and peace. Granted, security plays a role in every state, but security cannot be used as a trump card nor can it be used to justify disproportionate responses to threats. Some security concerns pertaining to migration are warranted but right-wing populists play on the fears of the electorate by framing security as the predominant lens for viewing questions relating to borders.

Right-wing populists cannot be blamed for the securitisation of migration. Rather, they are merely a catalyst in a pre-existing discourse.

[11] There are other factors at play. For example, populist politicians may spend more time on the ground speaking with their constituents; they express the rage that large demographics of society feel towards the liberal system of globalisation; and people may feel drawn to more radical parties as the traditional left and right hover at the centre, resulting in a deficit of meaningful opposition. Furthermore, it may just be that many people still hold xenophobic bias.

Indeed, parties of different persuasions have long framed migration policy through security terminology. Lazaridis and Konsta (2015: 184) explain:

> Security concerns have topped western political agendas since the attacks of 9/11, ... Included among the non-military threats to state security is migration, the idea being that liberal migration regimes advance cross-border risks – for example, that of terrorism – while more restrictive regimes minimise such threats and improve national and societal security.

The EU itself has played into the securitisation of migration. The 2016 European Agenda on Migration links the control of migration to security by explicitly stating that migration and border management will be a component of Common Security and Defence Policy missions ongoing in Niger and Mali (Davitti 2019: 47).

Notwithstanding the pre-existence of the securitisation paradigm, it nonetheless can be argued that populist parties are unique in the extent to which they exploit the othering of migrants to further their own political agenda. Lazaridis and Konsta point out how Golden Dawn in Greece and the British National Party in the United Kingdom 'take advantage of the securitisation of migration' (Lazaridis and Konsta 2015: 185) and how, 'via populist actions, exclusionary practices are promoted through the construction of Otherness'(Lazaridis & Konsta 2015: 185). Right-wing populists could push the discourse even further to the right which could in turn lead to more brutal approaches to border management.

But how does the paradigm of securitisation translate into the militarisation of borders? Or more succinctly, how could the rise of populism lead to the militaristic implementation of new border technologies? At first glance it may seem that right-wing populists are opposed to technologies on the border. Right-wing populists are often associated with crude tangible measures, such as building physical border walls. For example, President Trump and Viktor Orbán, Prime Minister of Hungary, are famous proponents of wall building (McTague 2017). Moreover, populist movements harken back to imagined glory days and this atavism seems at odds with the progression of technology. However, this view is overly simplistic. The populist leader of the US, President Trump, has invested in additional border security including new emerging technologies, albeit only after the idea was promoted by other Republicans (Cowen 2019). This demonstrates that populists' border policy is not mutually exclusive with emerging technology. This conclusion is corroborated by the fact that populists rely heavily on social media to consolidate their support, as was discussed above.

It may be argued that the militarisation of the EU external border is already taking place. Private military and security companies are already reaping the benefits of a culture of fear (Davitti 2019), and right-wing populism serves to fan the flames of this fear. Kraska (2007: 503) defines militarisation as

> a set of beliefs, values, and assumptions that stress the use of force and threat of violence as the most appropriate and efficacious means to solve problems. It emphasises the exercise of military power, hardware, organisation, operations, and technology as its primary problem solving tools.

This phenomenon that is taking place on the EU border as 'security threats' (Behr 2013) are framed to justify militaristic security methods

(Davitti 2019: 38). One indication that the external border of the EU is being militarised is that European military contractors, including Thales, EADS, Finmeccanica and Talos, benefit from producing technological equipment for border security (Jones & Johnson 2016: 5). Furthermore, during the migration crisis civil society called out the military style approaches of Frontex (Buxton 2016).[12]

While right-wing populism grows increasingly popular, there simultaneously is a rise in border militarisation, partly as a result of securitised discourse. It is the contention of this article that this combination could increase the potential of migrants' human rights being abused via new technologies. That is, unless developments in border technologies are monitored and leaders are made accountable for when these developments compromise the dignity of any person.

7 Conclusion

The application of new technologies in our daily life is unstoppable. As seen in this article, it can be for the good and for the bad. Due to a lack of knowledge about the workings of algorithms and missing regulations regarding transparency, technology is applied without necessarily knowing what harm it can do. Groups, especially those that are not on the frontlines of the fourth revolution and participating in the coding process, are left behind when it comes to knowing how the algorithm perceives them. Usually groups that are already vulnerable are also targeted by the bodiless algorithm. The most targeted group are dark-skinned people, especially women. In the most defenceless situations, such as at border crossing points, when applying for asylum an algorithm can not only discriminate against someone, but also massively violate other human rights. Therefore, it is more important than ever to be critical of new technologies and not to use them only because we can produce these technologies.

We are currently experiencing a shift in how security policies are made around the world. This shift carries the paradox that in order to have more security, one must trade off one's privacy. The tools theoretically used to fight terrorism and crime are the same as those used to scrutinise civilians, while convincing them that such tools are necessary and indispensable. In the long run, even when there are security-privacy trade-offs, these must be carefully assessed and weighted. As we are watching how regions shift towards a risk management approach, we will potentially witness limitations to civil rights and liberties.

For better or for worse, technology travels faster than law. Some laws that regulate privacy and data protection were created in the 1970s, such as the US Privacy Act, and have been proven to be outdated and insufficient to protect citizens against undue interference by states, and even private companies, that analyse and store such data. Although laws regulating privacy protection in Europe are a favourable step towards more data security, the mere definition of consent may have to be amended

[12] It should be noted that the European Commission, in response to a parliamentary question, stated that Frontex bears no similarity to promoting the militarisation of the EU (Papadakis 2016; European Commission 2017).

worldwide. Until now, consent has operated as a legitimate basis for personal data processing and practice shows that this definition is not enough (Gonzalez Fuster 2018). The common understanding of consent needs to be revisited, as we know what happens when we agree to disclose certain types of personal information, but not what happens when we do not.

As of now, the EU is implementing adequate legal protection with Regulation (EU) 2018/1725. Until more advanced artificially-intelligent systems, such as dynamic algorithms, are applied in law enforcement, the regulation will not provide the needed protection that is required and it will only be a question of time until new types of machine discrimination occur or new ways of misusing the current technology are found. It could be that facial recognition systems will be used in a wide range of situations in the near future, such as to identify individuals at protests or in the context of border management. This can have negative effects: Individuals will be screened long before they arrive at the actual border and the decision about whether they are allowed to enter will be made in advance. This new way of using profiling may be justified through security and prevention reasons. In cases such as the Berlin truck bomber, hypothetically it could have prevented terrorist attacks and saved lives. However, in other circumstances, if policy makers decide to close borders due to predictions from algorithms, this might have negative effects, especially for the security of people travelling in large migration flows.

Alongside the legal framework, which must be up to date with technologies and include different means of application to prevent unlawful profiling and discrimination, there is also a need to fight bias and profiling on different levels in society, so as to prevent the feeding of human bias to algorithms. To the same end, algorithms have to be written by a heterogeneous team. Additionally, the algorithm should be trained using wider and more diverse datasets, gathered through different providers from all over the world. Furthermore, law enforcement units need to be diverse and specifically trained to become aware of their own biases and to learn how to regulate them. There is also a need for awareness about the shortcomings in algorithms. Summarily, a diverse society is a prerequisite. Diversity brings more knowledge, which results in more empathy. If that can be achieved, there automatically will be less bias in human decisions as well as less implemented bias in algorithms – therefore, greater data protection.

If the prospect of more diversity evokes hope about the potential positive human rights implications of border technology; then the shift in politics towards othering of migrants provides ample reason for pessimism. As was stated, populists may not have directly contributed to border policies but they do feed into the paradigm of securitisation. This article concludes with a warning. Going forward, technological solutions may seem like a more humane option than building physical barriers, but there are an array of human rights concerns associated with border technology, as laid out in this article. The aim of emerging border technology is not contradictory to the populist approach to borders. In fact, they can be complementary. If right-wing populist discourse continues to slowly push policy to the right in Europe, it increases the likelihood of border technologies being used in a manner that does not enshrine the dignity of migrants. As the EU gets ready to begin its new mandate, it is worth remembering that new border technologies do not exist in a vacuum. Rather, how they are applied reflects political agendas. This lesson is as true in other regional contexts as it is in the EU. Ultimately, technology will change the way in which borders are managed across the world. It will impact sovereignty, migration routes, freedom of expression, privacy, surveillance and more. For this reason, considerate leadership is needed. Furthermore, it is the responsibility of scholars, human rights professionals and the media to highlight these emerging technologies and the consequences they have on vulnerable groups.

References

Amoore L (2013) *The politics of possibility: Risk and security beyond probability* NC: Duke University Press

Anduril (nd) *The lattice platform*, available at https://www.anduril.com/lattice-ai (last visited 12 April 2019)

Angelescu I & Trauner F (2018) *10 000 border guards for Frontex: Why the EU risks conflated expectations* European Migration and Diversity Programme, available at http://www.epc.eu/documents/uploads/pub_8745_frontex.pdf?doc_id=2048 (last visited 10 April 2019)

Arnold C (2010) *TSA to expand use of full-body scanners* National Public Radio, available at https://www.npr.org/templates/story/story.php?storyId=122289282 (last visited 12 April 2019)

Balfour R (2016) 'Europe’s troublemakers The populist challenge to foreign policy' European Policy Centre, available at http://www.epc.eu/documents/uploads/pub_6377_europe_s_troublemakers.pdf?doc_id=1714> (last visited 16 April 2019)

Bartlett J ‘Why is populism booming? Today’s tech is partly to blame’ *The Guardian* 29 November 2018, available at https://www.theguardian.com/commentisfree/2018/nov/29/populism-tinder-politics-swipe-left-or-right-unthinkingly (last visited 18 April 2019)

Behr T et al (2013) ‘The maritime dimension of CSDP: Geostrategic maritime challenges and their implications for the European Union’ Study Directorate General for External Policies, European Parliament, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433839/EXPO-SEDE_ET(2013433839_EN.pdf (last visited 13 June 2019)

Bier D & Feeney M (2018) *Drones on the border: Efficacy and privacy implications* CATO Institute, available at https://www.cato.org/publications/immigration-research-policy-brief/drones-border-efficacy-privacy-implications (last visited 15 April 2019)

Biometrics and Technologies *Council of Europe*, available at https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Biometrics tech nologies_v2.pdf (last visited 10 April 2019)

Bowling B & Sheptycki JWE (eds) (2015) *Global policing and transnational law enforcement* Sage Publications Ltd

Bowling B, Marks A & Murphy C ‘Crime control technologies: Towards an analytical framework and research agenda’ in R Brownsword & K Yeung (eds)

Regulating technologies: Legal futures, regulatory frames, and technological fixes (2008) OR: Hart Publishing 41(2018)

Buolamwini J. & Gebru T 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) 81 *Journal of Machine Learning Research* 77, available at http://proceedings.mlr.press/v81/ (last visited 15 April 2019)

Broeders D 'A European "border" surveillance system under construction' in H Dijstelbloem & A Meijer (eds) *Migration and the new technological borders of Europe: Migration, minorities and citizenship* (2011) London: Palgrave Macmillan 40

Broeders D 'The new digital borders of Europe: EU databases and the surveillance of irregular migrants' (2007) 22 *International Sociology*, available at https://doi.org/10.1177/0268580907070126 (last visited 12 April 2019)

Cagle M & Ozer N 'Amazon teams up with government to deploy dangerous new facial recognition technology' *American Civil Liberties Union* 22 May 2018, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new (last visited 13 May 2019)

Ceyhan A 'Technologization of security: Management of uncertainty and risk in the age of biometrics' (2008) 5 *Surveillance and Society*, available at https://doi.org/10.24908/ss.v5i2.3430 (last visited 9 April 2019)

Chishti M & Bergeron C 'Post-9/11 policies dramatically alter the US' (2011) *Immigration Landscape*, Migration Policy Institute, available at https://www.migrationpolicy.org/article/post-911-policies-dramatically-alter-us-immigration-landscape (last visited 12 April 2019)

CNBC 'These virtual walls could be the cheaper and more effective answer to Trump's $5 billion border wall' (2018), available at https://www.cnbc.com/video/2018/12/14/this-border-town-doesnt-want-trumps-wall-but-a-silicon-valley-virtual-wall-could-stand-strong.html (last visited 14 April 2019)

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180

Cowen R 'Beyond Trump's wall: Congress tackles border security' *Reuters* 30 January 2019, available at https://www.reuters.com/article/us-usa-shutdown-negotiators/beyond-trumps-wall-congress-tackles-border-security-idUSKCN1PO1ON (last visited 23 April 2019)

Davitti D 'The rise of private military and security companies in European Union migration policies' (2019) 4 *Business and Human Rights Journal*

Department of Homeland Security (2005) 'Fact Sheet: Secure border initiative', available at www.dhs.gov/xnews/releases/press_release_0794.shtm (last visited 10 April 2019)

Deutsches Referenzzentrum für Ethik in den Biowissenschaften [DRZE] (2019) 'Genetische Daten' translated by author *DRZE*, April, available at http://www.drze.de/im-blickpunkt/praediktive-genetische-testverfahren/module/genetische-daten (last visited 6 April 2019)

Diaz de Mera Garcia Consuerga A 'Smarter borders for Europe' *European Parliament* 25 October 2017, available at https://www.youtube.com/watch?v=J5qljEodBMM (last visited 13 April 2019)

Donohue K 'Technological leap, statutory gap, and constitutional abyss: Remote biometric identification comes of age' (2012) *Georgetown University Law Review* 1, available at https://www.eff.org/pages/iris-recognition (last visited 15 April 2019)

Elbit Systems ‘Elbit Systems presents Groundeye™: A new revolutionary line of advanced EO ground surveillance systems for wide-area focused and persistent intelligence gathering’ (2016), available at https://elbitsystems.com/pr-new/elbit-systems-presents-groundeye/ (last visited 11 April 2019)

Elbit Systems (nd) ‘Company profile: Next is now’, available at https://elbitsystems.com/media/Next-is-Now_Booklet_General.pdf (last visited 18 April 2019)

Elbit Systems (nd) ‘Home’, available at https://elbitsystems.com/ (last visited 18 April 2019)

EU Travel Information and Authorisation System ‘ETIAS border security technologies’ (2017), available at https://etias.com/articles/etias-border-security-technologies (last visited 12 April 2019)

European Commission (nd) ‘Biometric data’, available at https://ec.europa.eu/home-affairs/content/biometric-data_en (last visited 14 April 2019)

European Commission 'Answer given by Mr Avramopoulos on behalf of the Commission' Parliamentary Questions: Question reference: E-007071/2016’ 11 January 2017, available at http://www.europarl.europa.eu/doceo/document/E-8-2016-007071-ASW_EN.html (last visited 19 April 2019)

European Commission (2016) *Communication from the Commission to the European Parliament and the Council on the state of play of implementation of the priority actions under the European Agenda on Migration* (COM(2016) 85 final edn)

European Commission (2018a) ‘EU budget: €4.8 billion in security funding for a Europe that protects’

European Commission (2018b) ‘EU budget: Commission proposes major funding increase for stronger borders and migration’, available at http://europa.eu/rapid/press-release_IP-18-4106_en.htm (last visited 10 April 2019)

European Commission Press Release Data Base ‘The European Agenda on Migration: EU needs to sustain progress made over the past 4 years’ (2019), available at http://europa.eu/rapid/press-release_IP-19-1496_en.htm (last visited 18 April 2019)

European Union Agency for Fundamental Rights (2018a) *Preventing unlawful profiling today and in the future: A guide* Luxembourg: Publications Office of the European Union

European Union Agency for Fundamental Rights (2018b) *BigData: Discrimination in data-supported decision making* Luxembourg: Publications Office of the European Union

Etzioni A ‘Happiness is the wrong metric: A liberal communitarian response to populism’ (2018) 11 *Library of Public Policy and Public Administration*, available at https://www.springer.com/gp/book/9783319696225 (last visited 13 June 2019)

Executive Office of the President of the United States (2019) ‘Stronger border security: 2019 Budget Fact Sheet’, available at https://www.whitehouse.gov/wp-content/uploads/2018/02/FY19-Budget-Fact-Sheet_Border-Security.pdf (last visited 11 April 2019)

Fleming ST, Madden JM & Usery EL ‘GIS applications for military operations in coastal zones’ (2009) *ISPRS Journal of Photogrammetry and Remote Sensing* 64, available at http://scholar.google.pt/scholar_url?url=https://pdfs.semanticscholar.org/79c4/c469c72ba3237ea89147b2dc3fd5dc05ec75.pdf&hl=en&sa=X&scisig=AAGBfm1Tp8D3eaolHKSkvp_mpFkmtf5-og&nossl=1&oi=scholarr (last visited 13 April 2019)

Franko Aas K '"Getting ahead of the game": Border technologies and the changing space of governance' in E Zureik & MB Salter (eds) *Global surveillance and policing: Borders, security, identity* (2005) UK: Willan Publishing194

Frontex (nd) 'Migratory Map', available at https://frontex.europa.eu/along-eu-borders/migratory-map/ (last visited 11 April 2019)

Gardiner B *O*'ff with your shoes: The brief history of airport security' (2013), available at https://www.wired.com/2013/06/fa_planehijackings/ (last visited 10 April 2019)

Gemalto (nd) 'DHS's automated biometric identification system IDENT – The heart of biometric visitor identification in the USA', available at https://www.gemalto.com/govt/customer-cases/ident-automated-biometric-identification-system (last visited 17 April 2019)

Greenwald G 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* 2013, available at https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (last visited 11 April 2019)

Goodwin M 'Right response understanding and countering populist extremism in Europe' (2011) *A Chatham House Report*, available at https://www.chathamhouse.org/sites/default/files/r0911_goodwin.pdf (last visited 16 April 2019)

Haggerty KD & Ericson R 'The surveillant assemblage' (2000) 51 *British Journal of Sociology*, available at https://www.uio.no/studier/emner/matnat/ifi/INF3700/v17/bakgrunnsnotat/the_surveillant_assemblage.pdf (last visited 8 April 2019)

Hendricks VF & Vestergaard M 'Reality lost: Markets of attention, misinformation and manipulation' Springer Open (2019), available at https://www.springer.com/gp/book/9783030008123#aboutBook (last visited 13 June 2019)

Johansson-Nogués E 'The EU's ontological (in)security: Stabilising the ENP area and the EU-self?' (2018) 53 *Cooperation and Conflict*

Hoffman M 'The future of border securing technology is here and it's terrifying' VICE (2016), available at https://www.vice.com/en_us/article/zngp34/the-new-frontiers-in-border-security-technology (last visited 13 April 2019)

IDEMIA (nd) 'Video investigation: Analyzing video data to accelerate investigations', available at https://www.idemia.com/video-investigation (last visited 13 April 2019)

Immigration & Checkpoints Authority 'Contactless, "breeze-through" immigration clearance trial at Tuas checkpoint' (2019), available at https://www.ica.gov.sg/news-and-publications/media-releases/media-release/contactless-breeze-through-immigration-clearance-trial-at-tuas-checkpoint (last visited 12 April 2019)

Johnson J 'One hundred naked citizens: One hundred leaked body scans' Gizmodo (2010), available at https://gizmodo.com/one-hundred-naked-citizens-one-hundred-leaked-body-sca-5690749?utm_medium=sharefromsite&utm_source=gizmodo_copy&utm_campaign=top (last visited 13 April 2019)

Jones R & Johnson C 'Border militarization and the rearticulation of sovereignty' (2016) 41 *Transactions of the Institute of British Geographers*

Koslowski R & Schulzke M 'Drones along borders: Border security UAVs in the United States and the European Union' (2018) 19 *International Studies Perspectives*, available at˙ https://doi.org/10.1093/isp/eky002 (last visited 18 April 2019)

Kraska PB 'Militarization and policing: Its relevance to 21st century police' (2007) *Policing* 1

Kyle J & Gultchin L 'Populists in power around the world' *Tony Blair Institute for Global Change* (2018), available at https://institute.global/insight/renewing-centre/populists-power-around-world (last visited 18 April 2019)

Latonero M 'Big data analytics and human rights' in MK Land (ed) *New technologies for human rights and practice* (2018) Cambridge University Press

Landgericht Berlin (2018) *Klaus Muller v Facebook*

Lazardis G & Konsta A (2015) *Identitarian populism: Securitisation of migration and the far right in times of economic crisis in Greece and the UK* London: Palgrave Macmillan

Levy S 'Inside Palmer Luckey's bid to build a wall' (2018), available at https://www.wired.com/story/palmer-luckey-anduril-border-wall/ (last visited 13 April 2019)

Lewington L. 'Inside border technology' BBC Click (2018), available at https://www.youtube.com/watch?v=laeSuws-mE0 (last visited 18 April 2019).

Long D & Barrios D (nd) 'CBP's eyes in the sky: CBP's tethered aerostats keep watch for trouble from 10,000 feet' US Customs and Border Protection, available at https://www.cbp.gov/frontline/frontline-november-aerostats (last visited 12 April 2019)

Luyten K & González Díaz S 'Legal migration to the European Union' European Parliamentary Research Service (2019), available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635559/EPRS_BRI(2019)635559_EN.pdf (last visited 19 April 2019)

Lyon D (2007) *Surveillance studies: An overview* UK: Polity Press

Mason M (nd) 'Biometric breakthrough: How CBP is meeting its mandate and keeping America safe' US Department of Homeland Security, available at https://www.cbp.gov/frontline/cbp-biometric-testing (last visited 16 April 2019).

Massé 'EU's "Smart Borders 2.0" increases risks of surveillance and privacy abuses' *Access Now* 2016, available at https://www.accessnow.org/smartborders/ (last visited 5 April 2019)

Marx GT 'Some conceptual issues in the study of borders and surveillance' in E Zureik & MB Salter (eds) *Global surveillance and policing: Borders, security, identity* (2005) UK: Willan Publishing 11

MAV-lab (nd) 'Research topics', available at http://mavlab.tudelft.nl/research-topics/ (last visited 17 April 2019)

McDonald JOE 'China bars millions from travel for "social credit" offences' *Associated Press* 2019, available at https://news.yhttps://www.apnews.com/9d43f4b74260411797043ddd391c13d8ahoo.com/china-blocks-travel-social-credit-offenses-113811546--finance.html (last visited 1 April 2019)

McFarland M 'Amazon shareholders call for halt of facial recognition sales to police' *CNN Business* 18 June 2018, available at https://money.cnn.com/2018/06/18/technology/amazon-facial-recognition/index.html (last visited 10 April 2019)

Mctague T 'Hungary hardens immigration line' *Politico* 13 February 2017, available at https://www.politico.eu/article/hungarys-new-hardline-immigration-scheme-viktor-orban-refugees-migration-crisis-europe/ (last visited 20 April 2019)

Meyers DW 'Does "smarter" lead to safer? An assessment of the border accords with Canada and Mexico' Migration Policy Institute (2003), available at https://www.migrationpolicy.org/research/does-smarter-lead-safer-assessment-border-accords-canada-and-mexico?pdf=6-13-0~1.pdf (last visited 11 April 2019)

Mittelstadt M et al 'Through the prism of national security: Major immigration policy and program changes in the decade since 9/11' Migration Policy Institute

(2011), available at https://www.migrationpolicy.org/research/post-9-11-immigration-policy-program-changes (last visited 10 April 2019)

Moura P & Garcia-Navarro L ‘Brazil looks to build a 10,000-mile virtual fence’ National Public Radio (2013), available at https://www.npr.org/sections/parallels/2013/05/16/184524306/brazil-looks-to-build-a-10-000-mile-virtual-fence (last visited 15 April 2019)

Mozur P ‘Inside China's dystopian dreams: AI, shame and lots of cameras’ *The New York Times* 2018, available at https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html (last visited 1 April 2019)

Mozur P ‘One month, 500,000 face scans: How China is using AI to profile a minority’ *The New York Times* 14 April (2019), available at https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (last visited 14 April 2019)

National Ocean Service ‘What is LIDAR?’ National Oceanic and Atmospheric Administration (2018), available at https://oceanservice.noaa.gov/facts/lidar.html (last visited 12 April 2019)

Neville D, Sy D & Rigon A 'On the frontline: The hotspot approach to managing migration' Policy Department for Citizen's Rights and Constitutional Affairs European Parliament (2016), available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556942/IPOL_STU(2016)556942_EN.pdf (last visited 18 April 2019)

Nissenbaum H (2010) *Privacy in context technology, policy, and the integrity of social life* Stanford, CA: Stanford University Press

Nixon R ‘On the Mexican border, a case for technology over concrete’ *New York Times* 20 June 2017, available at https://www.nytimes.com/2017/06/20/us/politics/on-the-mexican-border-a-case-for-technology-over-concrete.html?module=inline (last visited 13 April 2019)

Northrop Grumman ‘Northrop Grumman showcases comprehensive security solutions at ASIS International’ (2004), available at https://news.northropgrumman.com/news/releases/northrop-grumman-showcases-comprehensive-security-solutions-at-asis-international (last visited 12 April 2019)

Nowrasteh A ‘The cost of the border wall keeps climbing and it’s becoming less of a wall’ Cato Institute (2019), available at https://www.cato.org/blog/cost-border-wall-keeps-climbing-its-becoming-less-wall (last visited 11 April 2019)

OHCHRa ‘The principle of *non-refoulement* under international human rights law’ (2018), available at https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/Protection.pdf (last visited 18 April 2019)

OCHRb ‘What do we mean by “protection” for migrants?’ (2018), available at https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/Protection.pdf (last visited 18 April 2019)

Office of Communications ‘Unravelling a butterfly’s aerial antics could help builders of bug-size flying robots’ John Hopkins University (2012), available at https://releases.jhu.edu/2012/02/01/butterfly-study-could-help-builders-of-bug-size-flying-robots/ (last visited 17 April 2019)

Office of Inspector General ‘CBP has not ensured safeguards for data collected using unmanned aircraft systems’ Department of Homeland Security (2018), available at https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-79-Sep18.pdf (last visited 17 April 2019)

Office of Inspector General ‘HHS OIG issue brief: Separated children placed in Office of Refugee Resettlement Care’ US Department of Health & Human Resources (2019), available at https://oig.hhs.gov/oei/reports/oei-BL-18-00511.pdf (last visited 15 April 2019)

Osborne Clarke 'Profiling and automated decision-making under GDPR' *Osborne Clarke* 5 September (2018), available at https://www.osborneclarke.com/insights/profiling-and-automated-decision-making-under-gdpr/ (last visited 6 April 2019)

Panetta G 'The US border patrol could be facing a lawsuit after 2 US citizens say they were detained for speaking Spanish' *Business Insider* (2018), available at https://www.businessinsider.com/border-patrol-racial-profiling-lawsuit-2018-5/ (last visited 12 June 2019)

Papadakis K 'Subject: "Militarisation of the EU" by the European border and coast guard' Parliamentary', Question to the Commission Question for written answer E-007071-16 to the Commission 26 September (2016), available at http://www.europarl.europa.eu/doceo/document/E-8-2016-007071_EN.html (last visited 19 April 2019)

Papernot N et al (2017) *Practical black-box attacks against machine learning* Cornell University, available at https://arxiv.org/pdf/1602.02697.pdf (last visited 13 April 2019)

Pasquino G 'Populism in democracy' in D Albertazzi & D McDonnell *Twenty first century populism: The spectre of Western European democracy* (2007) Hampshire: Palgrave Macmillian, available at https://books.google.es/books?hl=en&lr=&id=K2mADAAAQBAJ&oi=fnd&pg=PP1&ots=p8nr_PvWMG&sig=Sy5m4djHKNyEB57D8ve7REtaS10&redir_esc=y#v=onepage&q&f=false (last visited 16 April 2019)

Pickering S & Weber L 'Borders, mobility and technologies of control' in S Pickering & L Weber (eds) *Borders, mobility and technologies of control* (2006) Netherlands: Springer 1

Politifact at the Poynter Institute (2017) 'Triple ICE enforcement', available at https://www.politifact.com/truth-o-meter/promises/trumpometer/promise/1440/triple-ice-enforcement/ (last visited 17 April 2019)

Portilho T 'Our blind faith in AI is catching up to us' *Gulf Today* 27 March 2019, available at https://www.gulftoday.ae/opinion/2019/03/27/our-blind-faith-in-ai-is-catching-up-to-us (last visited 19 April 2019)

Quanergy Systems 'Quanergy Explains Solid State LiDAR' YouTube 2018, available at https://www.youtube.com/watch?v=eiu_V4a6vm4 (last visited 12 April 2019)

Quanergy Systems (nd) 'Mapping', available at https://quanergy.com/mapping/ (last visited 11 April 2019)

Raytheon (nd) 'JLENS', available at https://www.raytheon.com/capabilities/products/jlens (last visited 13 April 2019)

Reed J 'Israel extends its high-tech barriers I FT World' *Financial Times* (YouTube) (2016), available at https://www.youtube.com/watch?v=X9fe4m0UAg4 (last visited18 April 2019).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Ring T (ed) 'Frost and Sullivan forecasts expansion of border control biometrics' (2013) *Biometric Technology Today* 4, available at https://doi.org/10.1016/S0969-4765(13)70069-9 (last visited 12 April 2019)

Roth K. 'The dangerous rise of populism: Global attacks on human rights values' Human Rights Watch: World Report (2017), available at https://www.hrw.org/world-report/2017/country-chapters/dangerous-rise-of-populism (last visited 16 April 2019)

Ruiz Benedicto A & Brunet P 'Building walls: Fear and securitization in the European Union' TNI (2018), available at https://www.tni.org/en/publication/building-walls (last visited 8 April 2019)

Schengen Visa Info (2018) *Schengen Visa statistics for consulates – 2017*, available at https://www.schengenvisainfo.com/statistics/visa-statistics-2017/ (last visited 17 April 2019)

Schwab K 'The Fourth Industrial Revolution: What it means, how to respond' World Economic Forum (2016), available at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (last visited 17 April 2019)

Snow J 'Amazon's face recognition falsely matched 28 members of congress with mugshots' American Civil Liberties Union 26 July 2018, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (last visited 15 April 2019)

Stone P & Gordon G 'Cell signal puts Cohen outside Prague around time of purported Russian meeting' 18 April 2019, available at https://www.mcclatchydc.com/news/investigations/article219016820.html (last visited 16 June 2019)

Spotzi SD & Friedewalt M 'Aligning security and privacy' in *Surveillance, privacy and security* (2018) Routledge

The Alan Turing Institute Data Ethics Group and the Independent Digital Ethics Panel for Policing (2017) *Ethics Advisory Report for West Midlands Police*, The Alan Turing Institute Data Ethics Group, available at https://www.turing.ac.uk/sites/.../turing_idepp_ethics_advisory_report_to_wmp.pdf (last visited 15 April 2019)

The Economic Times 'Modi government plans 24X7 virtual fence along Indo-Pak border' 13 July 2018, available at https://economictimes.indiatimes.com/news/defence/modi-government-plans-24x7-virtual-fence-along-indo-pak-border/articleshow/59969417.cms (last visited 11 April 2019)

Transport Security Administration 'TSA biometrics roadmap for aviation security & the passenger experience' (2018), available at https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf (last visited 5 April 2019)

Travis A & Stewart H 'UK to pay extra £44.5m for Calais security in Anglo-French deal' *The Guardian* 18 January 2018, available at https://www.theguardian.com/politics/2018/jan/18/uk-to-pay-extra-445m-for-calais-security-in-anglo-french-deal (last visited 10 April 2019)

US Air Force Recruiting 'US air force micro air vehicles' YouTube (2015), available at https://www.youtube.com/watch?time_continue=77&v=hPS9FFRUXo0 (last visited 16 April 2019)

US Immigration and Customs Enforcement 'Who we are' (2018), available at https://www.ice.gov/about (last visited 12 April 2019)

US Government Accountability Office 'Report to congressional requesters: Secure border initiative: DHS needs to strengthen management and oversight of its prime contractor' (2010), available at https://www.gao.gov/new.items/d116.pdf (last visited 13 April 2019)

US Customs and Border Protection (nd) 'Trusted traveller programs: Frequently asked questions', available at https://ttp.cbp.dhs.gov/faq (last visited 12 April 2019)

Vallet E (2016) *Borders, fences and walls: State of insecurity?* NY: Routledge

West Midlands Police (nd) 'Data driven insight & data science capability for UK law enforcement', available at http://www.excellenceinpolicing.org.uk/wp-content/uploads/2017/10/EIP17_2-5_Utilising_Data_Science.pdf (last visited 12 April 2019)

Wodinsky S 'Palmer Luckey's border control tech has already caught dozens of people' *The Verge* (2018), available at https://www.theverge.com/2018/6/11/17448552/border-control-tech-security-lattice-palmer-luckey (last visited 12 April 2019)

Wood M 'Some quick thoughts on the public discussion regarding facial recognition and Amazon Rekognition this past week' *AWS Amazon Machine Learning Blog* 1 June 2018, available at https://aws.amazon.com/de/blogs/machine-learning/some-quick-thoughts-on-the-public-discussion-regarding-facial-recognition-and-amazon-rekognition-this-past-week/ (last visited 18 April 2019)