Submission to the 'UN Working Group on the use of mercenaries' on the role of private companies in immigration and border management and the impact on the rights of migrants

March 2020

privacyinternational.org

March 2020

Table of Contents

Privacy International's submission on role of private military and security companies in immigration and border management and the impact on the protection of the rights of all migrants.

Privacy International (PI) welcomes the call of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination on the role of private military and security companies in immigration and border management and the impact on the protection of the rights of all migrants.

The issues highlighted in the call for submissions are ones that PI has been investigating, reporting and monitoring as part of our campaigns demanding a humane approach to migration[1] and challenging the drivers of surveillance[2] amongst other domains of work that PI focused on exposing corporate and government data exploitation and surveillance.

This submission builds on PI's research and reporting highlighting examples of the involvement of private companies in immigration and border management sectors. After some introductory remarks it provides information on specific companies working on every step of the way. It then provides an overview of how ongoing practices amount to serious violations of the right to privacy of migrants and as a result facilitate violations of other human rights as well.

Introduction

To respond to migration flows – voluntary or forced – governments worldwide have prioritised an approach to immigration that criminalises the act of migration and focuses on security. Legal status controls are embedded at various moments of migrants' lives. It is no longer about physical national borders, but we are seeing the externalisation of borders with the transfer of border management to third countries and digital borders, i.e. digital portals and databases.

Increasingly these approaches have been formalised and coordinated as part of a broader strategy to digitise immigration enforcement. Large amounts of data are being requested from migrants, from their fingerprints to their digital data trails, while they are often put in a situation of constant surveillance, to identity their credibility and worthiness, and to monitor, track, and profile them. Life-changing decisions are being made on the basis of the data being collected but also inferred and observed, and yet there are limited safeguards in place to regulate and oversee the use of tech and data processing in immigration processes.

In this context, private military and security companies (PMSCs) have come to play essential roles in providing a variety of surveillance tech and data exploitation 'solutions' and services to governments. The interjection of for-profit actors such as surveillance companies offering

1 PI, Protecting Migrants at Borders and beyond, https://privacyinternational.org/protecting-migrants-borders-and-beyond (accessed 19 March 2020).
2 PI, Challenging the Drivers of Surveillance, https://privacyinternational.org/challenging-drivers-surveillance (accessed 19 March 2020).

– what they present as – easy technological solutions into immigration enforcement mechanisms, which is a highly complex sector, is inherently dangerous. Millions of people being forced to migrate because of war, persecution, and climate change is a call for urgent political and social action, not a business opportunity.

These companies are installing and often operating immigration and border surveillance systems with no consideration of the protections on the rights of migrations. They have infiltrated every step of the way with limited due regard or consideration of the impact of the surveillance technologies and data exploitations solutions they are introducing. They are not only profiting from the surveillance equipment they operate but they also use these opportunities to test and train new surveillance technologies.

Not only are such surveillance and data-driven immigration policies leading to discriminatory treatment of people and undermining peoples' dignity, but technological flaws also risk resulting in unfair and often erroneous decision making, particularly when automated. Compounded, these practices mean that migrants are bearing the burden of the new systems and losing agency in their migration experience, particularly when their fate is being put in the hands of systems driven by data processing and tech innovation.

1. Border monitoring services

There are few places in the world where an individual is as vulnerable as at the border of a foreign country.[3] Local and international travel is changing radically as concerns about terrorism and migration increase. Security agencies require access to travellers' information before they leave their homes, compulsory identification of travellers now includes the collection of fingerprints and facial images, and secret watchlists, dossiers and profiles are being developed. These policies and procedures are extremely costly, the potential for abuses and miscarriages of justice is high, and the benefits are debatable.

Some of the main issues we wanted to raise as part of the role of PMSCs in immigration in the management of border services include the development, maintenance and operation of advanced technologies, training and equipment to authorities to implement externalisation of borders, air/land/maritime surveillance.

1.1. Surveillance of borders: Building digital borders

Over the course of our work we have recorded and exposed instances of companies being involved in the provision of surveillance systems at the borders. Here are some examples.

As calls for a 'secure southern border' have been amplifying in the US by politicians, experts, and Silicon Valley techies are coming out in force to proffer swanky digital solutions in the

[3] PI, Tech at the Border, https://privacyinternational.org/taxonomy/term/703 (accessed 19 March 2020).

place of 30-foot steel slats or concrete blocks.[4] One such company is **Anduril Industries**, named after a sword in Lord of the Rings, which represents a symbol of hidden power.

In early 2019, the Washington Post reported that Anduril Industries had landed a contract with US Customs and Border Protection (CBP) to expand its digital border security system in California.[5]

Anduril's 'solution' for border security in the US is based on drones, sensors, Artificial Intelligence (AI), and machine vision. At present, the public remains in the dark about how such a border security system will operate in practice. Given the intrusiveness of Anduril's system, PI has written to Anduril and asked the company to provide basic information about how the system works.[6] The system appears to have the potential to affect those entering or exiting the US, those who approach the border, as well as those who happen to live next to Anduril's border infrastructure.

The Tohono O'odham Nation's reservation which marks Arizona's border with the Mexican state of Sonora has been under surveillance for many years already with different systems in place through the use of drones, cameras and censors.[7] However, the surveillance will be heightened with US CBP constructing 10 surveillance towers capable of continuously monitoring every person and vehicle within a radius of up to 7.5 miles.

It was reported that: *"The tower will be outfitted with high-definition cameras with night vision, thermal sensors, and ground-sweeping radar, all of which will feed real-time data to Border Patrol agents at a central operating station in Ajo, Arizona. The system will store an archive with the ability to rewind and track individuals' movements across time — an ability known as 'wide-area persistent surveillance.'"*[8] It was reported that the US CBP agency was working with an Israeli Military contractor, **Elbity systems**, Israel's largest military company, to build the towers.

The chilling effect of the threat of such surveillance has already been reported by researchers from the University of Arizona and Earlham College who published a study in January 2020 where they found that as a result of the building of the towers along the border, many migrants were forced to explore new ways to cross pushing them to more dangerous routes leading to deaths from dehydration, exhaustion, and exposure.[9]

---

4 PI, "The Questions the New Company Vying for Border Dominance in the US Needs to Answer", 15 February 2019, https://privacyinternational.org/long-read/2731/questions-new-company-vying-border-dominance-us-needs-answer (accessed 19 March 2020).

5 Cat Zakrzewski, "The Technology 202: Trump Wants a Border Wall. One of His Biggest Supporters in Tech Is Expanding a Virtual One", *The Washington Post*, 5 February 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/02/05/the-technology-202-trump-wants-a-border-wall-one-of-his-biggest-supporters-in-tech-is-expanding-a-virtual-one/5c5884b71b326b66eb098610/ (accessed 19 March 2020).

6 *ibid.*

7 Will Parrish, "The U.S. Border Patrol and an Israeli Military Contractor Are Putting a Native American Reservation Under "Persistent Surveillance"", *The Intercept*, 25 August 2019, https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance/ (accessed 19 March 2020).

8 *ibid.*

9 Samuel Norton Chambers, Geoffrey Alan Boyce, Sarah Launius and Alicia Dinsmore, "Mortality, Surveillance and the Tertiary "Funnel Effect" on the U.S.-Mexico Border: A Geospatial Modeling of the Geography of Deterrence", *Journal of Borderlands Studies* (2019), https://doi.org/10.1080/08865655.2019.1570861 (accessed 19 March 2020), pp 1–26.

1.2. *Border Externalisation*

"Border Externalisation", the transfer of border controls to foreign countries, has in the last few years become the main instrument through which the European Union (EU) seeks to stop migratory flows to Europe. Similar to the strategy being implemented under Trump's administration, it relies on utilising modern technology, training, and equipping authorities in third countries to export the border far beyond its shores.[10] PMSCs and the broader surveillance industry complex are playing an essential role in the process.

Their involvement is enabled by the adoption of *ad hoc* funds, like the controversial "EU-Turkey deal", an agreement which saw €6 billion given to Turkey in exchange for its commitment to seal its border with Greece and Syria, and which has had dramatic implications for peoples' human rights.[11] Another is the EU Trust Fund for Africa (EUTF), a supposedly-emergency fund created in 2015 totalling € 4.3 billion by the end of 2018 – over € 4 billion of which comes from EU development aid and cooperation funds.[12]

Most of these instruments will be part of the new Neighbourhood, Development and International Cooperation Instrument (NDICI), a proposed external instrument under the EU's next budget for 2021-2027 (known as the Multiannual Financial Framework).[13]

We reported how this policy of "Border Externalisation" was being deployed in various countries including Libya, Niger and Egypt.[14] Whilst it there is little information about who is providing some of the technological tools provided as part of different programmes, it is most likely that these are provided in part if not completely by the private sector. Programmes include the strengthening the role of the Libyan Coast Guard to intervene and intercepting migrants at sea, the creation of a Mobile Border Post (MBP), a new mobile border checkpoint for Niger authorities developed with Canadian funds, or a border police training program for all of Africa (ITEPA project).

In particular in the case of Niger, PI raised concerns about how Niger had become the main recipient of an EU emergency trust fund to tackle the "root causes" of migration.[15] While EU programme documents state that the Fund has provided a wiretapping centre, sophisticated

---

10 P, "Here's the Surveillance the US Exports to Central America as Aid - And It's Surviving Trump's Cuts", 29 July 2019, https://privacyinternational.org/news-analysis/3011/heres-surveillance-us-exports-central-america-aid-and-its-surviving-trumps-cuts (accessed 19 March 2020).

11 Daniele Biella, "L'accordo Ue-Turchia viola i diritti umani, ci sono le prove", *Vita*, 28 June 2016, http://www.vita.it/it/article/2016/06/28/laccordo-ue-turchia-viola-i-diritti-umani-ci-sono-le-prove/139960/ (accessed 19 March 2020).

12 PI, "Policy Briefing - The Future of the EU Trust Fund for Africa", 18 September 2019, https://privacyinternational.org/advocacy/3220/policy-briefing-future-eu-trust-fund-africa (accessed 19 March 2020).

13 PI, "Policy Briefing - The EU Neighbourhood, Development and International Cooperation Instrument", https://privacyinternational.org/advocacy/3219/policy-briefing-eu-neighbourhood-development-and-international-cooperation-instrument (accessed 19 March 2020).

14 PI, "New Report Underlines the EU's Strategy in the War on Migration: Border Externalisation", 18 September 2019, https://privacyinternational.org/news-analysis/3224/new-report-underlines-eus-strategy-war-migration-border-externalisation (accessed 19 March 2020).

15 PI, "Europe's Shady Funds to Border Forces in the Sahel", 18 September 2019, https://privacyinternational.org/news-analysis/3223/europes-shady-funds-border-forces-sahel (accessed 19 March 2020); and PI, "The European Chase for Saharan Smugglers", 28 January 2020, https://privacyinternational.org/long-read/3347/european-chase-saharan-smugglers (accessed 19 March 2020).

mobile phone surveillance system known as an IMSI Catcher, surveillance drones, and other surveillance software the border police in Niger, it is not known which private security company they sourced it from.[16] The case of the **GAR-SI** (Quick Action and Surveillance Groups in the Sahel), a security programme funded through the EU Trust Fund for Africa, shows that this might include drones, night vision equipment and photo cameras. The acquisition and operation of this equipment most likely involves the deployment of PMSCs in the broader surveillance complex. They will often be the only ones knowing which technology exists and how to use it.

1.3. Use of drones

In August 2019, it was reported by the Observer that the EU had invested over $115 million in Israeli-made unmanned drones to police the Mediterranean Sea.[17] The contracts providing this equipment were between Frontex, the EU's border and coastguard agency, and the European Maritime Safety Agency, the Israeli arms companies **Elbit Systems**, and state-owned **Israel Aerospace Industries**. Reportedly, they involved two Israeli-made unmanned drones, models. The Hermes model is made by Elbit Systems, Israel's biggest privately-owned arms manufacturer. The second model, the Heron, is produced by Israel Aerospace Industries, a state-owned company. "Both models were developed for use in combat missions in the occupied Palestinian territory of Gaza."[18]

2. Screening and/or determination of asylum or other claims for protection under international law

We have seen the involvement of companies in a variety of ways in the screening and/or determination of asylum or other claims for protection. Some of the main areas we have observed are outlined below.

2.1. Biometrics processing

As with many other sectors, we have seen the deployment of biometric systems in immigration and border management mechanisms. In these mechanisms, biometric technology is provided by companies to serve a variety of purposes including in screening and/or determination of asylum as part of age and origin verification, as well registration, authentication and verification of identity.

For example, **ATOS** company has been providing biometric technology for age verification and determination origin. ATOS is a European multinational information technology service and

---

16 Fonds fiduciaire d'urgence de l'union européenne en faveur de la stabilité et de la lutte contre les causes profondes de la migration irrégulière et du phénomène des personnes déplacées en Afrique, https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf, p 9

17 Daniel Howden, Apostolis Fotiadis, and Antony Loewenstein, "Once Migrants on Mediterranean Were Saved by Naval Patrols. Now They Have to Watch as Drones Fly Over", *The Observer*, 4 August 2019, https://www.theguardian.com/world/2019/aug/04/drones-replace-patrol-ships-mediterranean-fears-more-migrant-deaths-eu (accessed 19 March 2020).

18 *Ibid.*

consulting company headquartered in Bezons, France.[19] Since 2017, ATOS provided the German Federal Office for Migration and Refugees a new Identity Management System (IDM-S) for immigrants.[20]

In 2003, the Identification of applicants (EURODAC) was adopted and set-up an EU asylum central fingerprint database.[21] It is to this central database that the fingerprints of any person seeking asylum over the age of 14[22] anywhere in the European get transmitted. It is used for fingerprint comparison evidence to assist with determining the Member State responsible for examining an asylum application made in the EU to ensure compliance with the Regulation (EU) No. 604/2013 ('the Dublin Regulation')[23] which requires those seeking asylum to submit their claim in the first country of the EU they enter. The database holds other pieces of personal information, including country of origin, sex, and date and place of apprehension or asylum application.

When it was first launched, **Cogent Systems**, acquired by Gemalto that was recently acquired by Thales, won the contract to supply the Eurodac Automated Fingerprint Identification System (AFIS) to implement EURODAC Regulation. Gemalto Cogent still performs this contract today.[24]

2.2. Cellphone extractions

European countries are increasingly using smartphone surveillance to investigate asylum seekers. In Austria, Germany, Denmark, Norway, the United Kingdom, and Belgium, we have seen laws allowing for the seizure of mobile phones from applicants from which data is then extracted.[25]

There are various companies provide such tools but one marketing itself as the "global leader in digital intelligence".[26] is **Cellebrite.** Traditionally used to extract data from the phones of people under criminal investigation, Cellebrite is now marketing its digital extraction devices

---

19 ATOS, Homepage https://atos.net/en/ (accessed 19 March 2020).

20 Bernd Mainzer, "'Asylum Is a Fundamental Right; Granting It Is an International Obligation' – European Commission'" Atos (blog), 18 September 2018, https://atos.net/en/blog/asylum-fundamental-right-granting-international-obligation-european-commission (accessed 19 March 2020).

21 PI, "The EURODAC Debate: Do Asylum-Seekers Deserve Human Rights?", 12 December 2012, https://privacyinternational.org/blog/1424/eurodac-debate-do-asylum-seekers-deserve-human-rights (accessed 19 March 2020).

22 A new proposal aims to lower the age limit to 6 years old. European Commission, Identification of applicants (EURODAC), https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en (accessed 19 March 2020).

23 Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, OJ L 180, 29.6.2013, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=celex%3A32013R0604 (accessed 19 March 2020), pp 31–59.

24 Gemalto website, "EURODAC - EU Asylum Applicants & Border-Crossers (2019)", https://www.gemalto.com/govt/customer-cases/eurodac (accessed 19 March 2020).

25 Morgan Meaker, "Europe Is Using Smartphone Data as a Weapon to Deport Refugees", *Wired UK*, 2 July 2018, https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations (accessed 19 March 2020).

26 Cellebrite webstie, "Cellebrite Introduces Breakthrough Digital Intelligence Platform", https://www.cellebrite.com/en/press/cellebrite-introduces-breakthrough-platform-that-revolutionizes-digital-intelligence/ (accessed 19 March 2020).

at authorities interrogating people seeking asylum.[27] The Israel-based company, a subsidiary of Japan's Sun Corporation, markets forensic tools which empower authorities to bypass passwords on digital devices, allowing them to download, analyse, and visualise data. Already outside the context under consideration here, one should consider that in Bahrain, Cellebrite's technology was reportedly used to extract conversations and data from Mohammed al-Singace, a political activist who was tortured in custody.[28]

The potential use of its product to investigate the digital lives of people seeking asylum was outlined by its VP of International Marketing in a pitch in 2018 in Morocco to government officials gathered from around the world. According to Cellebrite's salesperson, some "77% of refugees [sic] arrive without document", while 43% have a smartphone during their journey – insisting that in lieu of documents, a person's phone could be used to find out who they are, what they have been doing, where they have been, when, and ultimately why they are seeking asylum.[29]

Smartphones are vital for migrants – not just for keeping in touch, but because they are a key means by which they plan journeys and obtain information, including information on safe routes and potential risks such as dangerous smugglers, as well as information about accessing vital services when they arrive in a safe country.

Our main concerns include the legality of such policies. Under international human rights law, surveillance is an interference with the right to privacy, and therefore needs to abide by fundamental principles designed to safeguard against arbitrary searches which undermine democracy and people's fundamental rights. For example, any surveillance needs to be necessary and proportionate to the overall aim, and not be discriminatory based on characteristics such as race or birth origin.
This means that national laws requiring invasive surveillance measures can still be a violation of international law if they do not meet these standards.

We are also concerned by the lack of process to obtain meaningful, freely given and unambiguous consent as when it comes to consent, it is more complicated than simply acquiring a person's permission. As articulated under European data protection regulations, for example, consent is not freely given and informed if the entity requesting it is in a position of power over the individual or fear adverse consequences so that they are not in a position to disagree. If a person fears being denied asylum and deported if they don't hand over their phone, it does not constitute "consent". It can hardly be said that consent is fully informed or unequivocal if the person concerned is unlikely to have full knowledge of the scope or types of information that may be extracted and retained.

Finally, the assumption that data obtained from digital devices leads to reliable evidence is flawed. If a person claims certain information is true, and there exists information on their smartphone suggesting otherwise, it is not evidence that they are lying. They may have

---

[27] PI, "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers", 3 April 2019, https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers (accessed 19 March 2020).
[28] Bahrain Watch - AmanaTech., "Cellebrite Forensics Technology", https://bahrainwatch.org/amanatech/en/investigations/cellebrite (accessed 19 March 2020).
[29] See above note 27.

swapped phones, they may have accessed certain sites or liked certain social media activity for a whole variety of reasons, and they may have been in touch with people whose name spelling appears on watchlists for a whole variety of reasons. And just because a person fleeing persecution from government forces does not want an agent flicking through their photos and messages, it also doesn't mean that they are automatically lying.

The use of such extraction tools, which are supposed to be used in exceptional circumstances, is part of a broader trend of aiming surveillance and other security technology at asylum seekers and migrants, often on scientifically dubious grounds. In Europe, this includes the use of technology which supposedly identifies if a person is lying based on their 'micro-gestures', a person's origin based on their voice, and their age based on their bones.[30]

2.3. Hacking

Various countries are also resorting to government hacking[31] as part of immigration enforcement techniques. In February 2019, the Swedish parliament approved a new law permitting law enforcement to hack the devices of undocumented migrants and migrants without an official permission to remain in the country.[32] A bit earlier, in 2018, it was reported by the Observer following confirmation from the Home Office that following amendments to the Police Act 1997 since 2013 immigration officials have been granted the power to "property interference, including interference with equipment".[33] Such powers included the ability to plant a listening device in a home, car or detention centre, as well as hacking into phones or computers.

Using such intrusive powers to target those remaining illegally in a country, without other reasonable suspicion, constitutes a disproportionate interference with their privacy. Underlying such power is a presumption that those migrants are staying by choice and intend to commit serious crimes. Individual circumstances vary and such assumptions are dangerous as they feed into racist and nationalistic narratives.[34] As well as raising privacy concerns which PI has documented extensively[35], there are concerns that these powers could undermine lawyer-client confidentiality in sensitive immigration and asylum cases.

---

30 Melanie Ehrenkranz, "An AI Lie Detector Is Going to Start Questioning Travelers in the EU", *Gizmodo*, 31 October 2018, https://gizmodo.com/an-ai-lie-detector-is-going-to-start-questioning-travel-1830126881 (accessed 19 March 2020); "Automatic Speech Analysis Software Used to Verify Refugees", Dialects, DW, 17 March 2017, https://www.dw.com/en/automatic-speech-analysis-software-used-to-verify-refugees-dialects/a-37980819 (accessed 19 March 2020); Miranda Aldersley, "Young Migrants Will Have to Undergo X-Ray Tests to Establish Age", *Mail Online*, 22 March 2019, https://www.dailymail.co.uk/news/article-6839551/Young-migrants-undergo-X-ray-tests-BONES-establish-age-France.html (accessed 19 March 2020).

31 PI, "Government Hacking", https://privacyinternational.org/taxonomy/term/37 (accessed 19 March 2020).

32 Alex Henrik, "Lagrådet säger ja till hemlig dataavläsning", *Femte juli,* 18 November 2019, https://femtejuli.se/2019/11/18/lagradet-sager-ja-till-hemlig-dataavlasning/ (accessed 19 March 2020).

33 Mark Townsend, "Revealed: Immigration Officers Allowed to Hack Phones", *The Observer*, 10 April 2016, https://www.theguardian.com/world/2016/apr/10/immigration-officials-can-hack-refugees-phones (accessed 19 March 2020).

34 PI, "New Swedish Draft Proposal for Government Hacking Powers Violates Human Rights Standards", 28 November 2019, https://privacyinternational.org/news-analysis/3291/new-swedish-draft-proposal-government-hacking-powers-violates-human-rights (accessed 19 March 2020).

35 See above note 31.

The role of PMSCs in the process cannot be overstated. While some sophisticated intelligence or security agencies can develop and use their own tools to hack into devices, there also exists an industry specialising in developing and selling such tools to government agencies which cannot. For example, one of the most high profile companies in the sector is **Hacking Team,** an Italian surveillance company which sold invasive surveillance technologies to law enforcement and intelligence agencies and is associated with attacks on political dissidents, journalists and human rights defenders across the globe. Though there is no evidence that its product was used as part of immigration enforcement , evidence has been published confirming its suspected deployment in at least 21 countries.[36] While these companies shield their customer lists from public scrutiny, it is foreseeable that some of their customers may include border control or immigration agencies.

3. Processing of visas and/or pre-departure screening at airports or other points of departure (e.g. related to carrier restrictions)

We have also seen the role by industry, including use of various intrusive surveillance techniques as part of visa processes and/or pre-departure screening at airports or other points of departure or at the border.

3.1. Social media intelligence (SOCMINT)

Over the last few years, we have seen governments across sectors including for immigration enforcement purposes resorting to social media intelligence (SOCMINT), the techniques and technologies that allow companies or governments to monitor social media networking sites (SNSs), such as Facebook or Twitter.[37] Some of these activities are undertaken directly by government themselves but in some instances, governments are calling on companies to provide them with the tools and/or knowhow to undertake this sort of activities.

In September 2010, Frontex, the European Border and Coast Guard Agency, published a call for tender to pay €400,000 to a surveillance company to track people on social media so that border guards "would have an understanding of the current landscape" as well as "a strategical warning system on changes such as the socio-political, economic or human security environment that could pose challenges to Frontex policies."[38] Though it is unclear whether private companies were involved, reportedly the European Asylum Support Office (EASO) monitored refugee networks to detect new routes and find smugglers[39], a practice that stopped after the European Data Protection Supervisor (EDPS) imposed a temporary ban.

---

[36] PI, "Briefing for the Italian Government on Hacking Team's surveillance exports", https://privacyinternational.org/sites/default/files/2018-02/Briefing%20for%20the%20Italian%20Government%20on%20Hacking%20Team's%20surveillance%20exports.pdf (accessed 19 March 2020).

[37] PI, "Social Media Intelligence", 23 October 2017, https://privacyinternational.org/explainer/55/social-media-intelligence (accessed 19 March 2020).

[38] 'ETendering - Data', 25 September 2019, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=5471 (accessed 19 March 2020).

[39] Alexander Fanta, "[Investigation] Data Watchdog Raps EU Asylum Body for Snooping", *EUobserver*, 9 December 2019, https://euobserver.com/investigations/146856 (accessed 19 March 2020).

The EDPS said the European Asylum Support Office has no legal basis for monitoring refugee routes on social media and imposed a temporary ban on the practice.[40]

In addition to gathering "data and analysis of relevant actors using social media: migrants; traffickers/smugglers", Frontex also wanted to monitor "civil society and diaspora communities in destinations (EU)." [41]

Following this announcement, PI set up an account on the procurement website, and asked them detailed questions to find out how they came to the conclusions they did, and if they had gone through the necessary checks to make sure their plan was legal.[42] These questions were based on a single legal instrument, the Regulation 2018/1725, which is the equivalent of the GDPR for EU institutions and is thus meant to regulate how EU bodies like Frontex process personal data. Similar to other questions, the agency would have had to publish the answers on the tender site. Instead of answering the questions, they decided to cancel the tender process. They told the journalist it was because of "the upcoming entry into force of the new European Border and Coast Guard Regulation."[43] But this doesn't seem credible, suggesting that the agency has only now become aware of the Regulation which governs its own mandate and proposed in 2018.

One of the companies collaborating with migration authorities is **Giant Oak**. The company, Giant Oak, markets itself to government and financial institutions and describes its Giant Oak Search Technology (GOST) as an "open source search and triage tool" that leverages open sources, social media, and the deep web to identify evidence of illicit activity and relevant information about entities of interest to clients.[44]

Their tool scrapes the web to pull in and search through vast amounts of information available online – such as news stories, blog posts, and images – as well as social media information. Layered on top of the search capability, the tool uses "sophisticated analytics scoring" to prioritise how results are shown, allows customers like ICE to search by key words, and provides a "dossier creation user interface".[45]

The company appears to have been working with ICE since 2014. In June 2017, the company was awarded a massive contract valued at over $37 million with ICE for open source and social media data analysis.[46] According to an analysis by PI, Giant Oak has made close to $45 million from its work with ICE.

---

[40] Formal consultation on EASO'ssocial media monitoring reports (case 2018-1083), European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf (accessed 19 March 2020).

[41] See above note 38.

[42] PI, "#PrivacyWins: EU Border Guards Cancel Plans to Spy on Social Media (for Now)", 19 November 2019, https://privacyinternational.org/node/3289 (accessed 19 March 2020).

[43] *Ibid.*

[44] OAK Website, GOST® (Giant Oak Search Technology), https://www.giantoak.com/product (accessed 19 March 2020).

[45] PI, "Who Supplies the Data, Analysis, and Tech Infrastructure to US Immigration Authorities?", 9 August 2018, https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities (accessed 19 March 2020).

[46] Federal Procurement Data System, https://www.fpds.gov/ezsearch/fpdsportal?q=%22giant+oak%22+DEPARTMENT_FULL_NAME%3A%22HOMELAND+SECURITY%2C+DEPARTMENT+OF%22+PIID%3A%22HSCEMD17D00001%22&s=FPDSNG.COM&templateName=1.5.1&indexName=awardfull&x=0&y=0&sortBy=SIGNED_DATE&desc=Y (accessed 19 March 2020).

3.2. *Passenger Name Records (PNR) screening*

The monitoring of Passenger Name Records (PNR) has been increasingly used to monitory migratory movements.[47] There are various companies which provide Passenger Name Records (PNR) screening services such **SITA**, a multinational information technology company providing IT and telecommunication services to the air transport industry. SITA provides a variety of services.[48] Among others, it offers iBorders GovernmentGateway, which delivers the traveller information to governments in order to understand who will be traveling to, from and through their country;[49] iBorders FastStart, which allows for real-time vetting of travellers by connecting traveller data (passengers and crew), visa systems and watch lists;[50] and the SITA Smart Path. The last one deserves a closer look.

SITA promotes it as its "most comprehensive **whole-journey identity** management solution".[51] It uses apparently digital biometric ID management technology and tracks the passengers throughout their journey. It aspires to replace passport and boarding pass checks in airports with facial recognition scans. In the process, it also integrates with government systems and databases to allow for immigration and border checks.

4. Management and security of immigration-related detention facilities

The privatisation of detention centres in Europe has been of increasing concern.[52]
As reported by Migreurope, this process is taking various forms. In the UK, the majority of migrant detention centres are managed by multinational security companies including **G4S, GEO group, Mitie, Serco, and Tascor**.[53] In Italy the management of detention centres and detainee care services have recently been outsourced to private companies such as the French company **GEPSA** (management of auxiliary prison services), a subsidiary of COFELEY.[54]

Further examples include the surveillance by the well-known private company, **G4S**, in 6 migrant detention centres in Greece since 2012.[55]

---

[47] The UN Counter-terrorism programme to build a PNR database involves the International Organisation for Migration (IOM). UN Counter-Terrorism Travel Programme Summary, Building the Capacity of Member States to Prevent, Detect and Investigate Terrorist Offenses and Related Travel by Using Advance Passenger Information (API) and Passenger Name Record (PNR) Data, https://www.un.org/cttravel/content/summary, (accessed 19 March 2020).
[48] SITA website, "How do I…Detect and intercept high risk travelers early and proactively?", https://www.sita.aero/solutions-and-services/sectors/governments/challenges/detect-and-intercept-high-risk-traverlers (accessed 19 March 2020).
[49] SITA website, iBorders® GovernmentGateway, https://www.sita.aero/solutions-and-services/solutions/iborders-governmentgateway (accessed 19 March 2020).
[50] SITA website,
iBorders® FastStart, https://www.sita.aero/solutions-and-services/solutions/iborders-faststart (accessed 19 March 2020).
[51] SITA website,
SITA Smart Path™, https://www.sita.aero/solutions-and-services/solutions/sita-smart-path (accessed 19 March 2020).
[52] Lydie Arbogast, "Migrant detention in the European Union: A thriving business", Rosa Luxemburg Stiftung, mgireurop, July 2016, https://www.migreurop.org/IMG/pdf/migrant-detention-eu-en.pdf (accessed 19 March 2020).
[53] *ibid*, p 22.
[54] *ibid*., p 28.
[55] Arbogast, note 52, p 40.

The reported impacts by Migreurope includes cutting costs and increasing profits to the detriment of detained migrants, poorer detention conditions, potential for increased violence against detainees, and turning migrants into captive labour force.

5. Collection of biometric data and use of private security technologies to support immigration and border management procedures

5.1. Building biometrics databases

As noted above, over the last few years we have seen a multitude of biometric systems in immigration and border management mechanisms. In these mechanisms, biometric technology is provided by companies to serve a variety of purposes including registration, verification and authentication.

Civipol, positions itself as the technical cooperation operator of the French Ministry of the Interior. It is part-owned by large arms producers as **Thales, Airbus and Safran**. Civipol is one of the executive partners of a project called 'Better Migration Management' implemented in the Horn of Africa.[56] In December 2016, Civipol was chosen to set-up and deploy databasis to fingerprint everyone in Mali and Senegal.[57] Going beyond fingerprinting, it is one of the two companies that are building a full biometric ID-system in Senegal.[58] It also implements a similar project in Côte d' Ivoire.[59] These projects are financed by the EUTF.[60] Their primary aim of these projects is to be able to identify irregular migrants from both countries who may be in Europe and then to deport them.[61]

As part of its research on foreign security assistance by law enforcement, military, and intelligence agencies, PI highlighted that the US State Department provides partner countries with the biometric traveller screening system developed by defence contractor **Booz Allen Hamilton** – the Personal Identification Secure Comparison and Evaluation System - to Burkina Faso, Cameroon, Chad, Djibouti, Ethiopia, Kenya, Mali, Niger, Tanzania, Uganda, Iraq, Jordan, Yemen, Maldives, Afghanistan, and Macedonia.[62]

---

[56] Mark Akkerman, Expanding the Fortress, The policies, the profiteers and the people shaped by EU's border externalisation programme, tni and Stop Wapenhandel, May 2018, https://reliefweb.int/sites/reliefweb.int/files/resources/expanding_the_fortress_-_1.6_may_11.pdf (accessed 19 March 2020).

[57] *ibid.*

[58] EU ETFA, "Programme d'appui au renforcement du système d'information de l'état civil et à la création d'un fichier national d'identité biométrique", https://ec.europa.eu/trustfundforafrica/region/sahel-lake-chad/senegal/programme-dappui-au-renforcement-du-systeme-dinformation-de-letat_en (accessed 19 March 2020).

[59] EU ETFA, "Contrat de réforme sectorielle / Appui à la réforme de l'état civil en Côte d'Ivoire", https://ec.europa.eu/trustfundforafrica/region/sahel-lake-chad/cote-divoire/contrat-de-reforme-sectorielle-appui-la-reforme-de-letat-civil_en (accessed 19 March 2020).

[60] See above note 12.

[61] For more information: EU ETFA, The 2017 Annual Report of the EU Emergency Trust Fund, 21 March 2018, https://ec.europa.eu/trustfundforafrica/all-news-and-stories/2017-annual-report_en (accessed 19 March 2020).

[62] PI, "Teach 'em to Phish: State Sponsors of Surveillance", July 2018, https://privacyinternational.org/sites/default/files/2018-07/Teach-em-to-Phish-report.pdf (accessed 19 March 2020).

As reported by PI in 2019, Trump administration has been cutting aid to Central America, including a surprise cut of approximately $500m in aid to the "Northern Triangle" countries of El Salvador, Guatemala, and Honduras,[63] and what is left of the funds is largely and deliberately being repurposed for spending on the US's own security interests.[64] One area which President Trump's attorney general claims will be spared from the cuts to the Northern Triangle is police aid - the provision of financial and technical assistance to law enforcement agencies, which includes the provision of surveillance capabilities.[65]

One such programme is the Biometric Identification Transnational Migration Alert Program (BITMAP). Passed in 2018, despite failing to require adequate privacy protections, it allows Immigration and Customs Enforcement (ICE) agents to provide biometric training and equipment to foreign agencies.[66] The collected data is then shared with US biometric databases, including a new system known as HART developed by arms company **Northrop Grumman**,[67] which according to a DHS presentation seen by PI will scoop up a whopping 180 million new biometric transactions per year by 2022.[68]

For example, under BITMAP, the State Department in Costa Rica spent nearly $60,000 last year on Jump Kits for capturing and sharing biometric data, according to US procurement records.[69] As of 2018, BITMAP was deployed to 14 countries, "with near-term plans to expand to additional countries."[70]

5.2. Databases management

One of the key functions that can be delegated to PMSCs is the management and maintenance of databases where public authorities store and handle troves of personal data of thousands of people. **T-rex** is an example of such company. It is a technology company that has contracts with the US Immigration and Customs Enforcement Agency (ICE) to 'modernise'

---

[63] See above note 10; Teresa Welsh, "Implementers, Missions in the Dark about Central America Assistance Cuts", *devex*, 17 May 2019 https://web.archive.org/web/20190517230358/https://www.devex.com/news/implementers-missions-in-the-dark-about-central-america-assistance-cuts-94914 (accessed 19 March 2020).

[64] Congressional Research Service, "U.S. Strategy for Engagement in Central America: Policy Issues for Congress, Updated 12 June 2019, https://www.hsdl.org/?view&did=826312 (accessed 19 March 2020).

[65] "Trump Will Not Cut Police Aid to Central America, Barr Says", *Reuters,* 16 May 2019, https://www.reuters.com/article/us-usa-immigration-centralamerica-idUSKCN1SM2II (accessed 19 March 2020).

[66] ACLU, ilrc, National Immigration Center, National Immigration Project of the National LAyers Guild, Re: Vote NO onH.R. 6439, the Biometric Identification Transnational Migration Alert Program (BITMAP) Authorization Act of 2018, 4 September 2018, https://web.archive.org/web/20190716015838/https:/www.aclu.org/sites/default/files/field_document/vote_recommendation_on_h.r._6439_the_bitmap_authorization_act_of_2018.pdf (accessed 19 March 2020).

[67] Stephen Mayhew, "US House Homeland Security Committee Advances Biometric Data Sharing Bill", Biometric Update, 30 July 2018, https://www.biometricupdate.com/201807/us-house-homeland-security-committee-advances-biometric-data-sharing-bill (accessed 19 March 2020).

[68] PI, "US Border Cops Set to Use Biometrics to Build a Line Up of the World", 25 October 2017, https://privacyinternational.org/news-analysis/648/us-border-cops-set-use-biometrics-build-line-world (accessed 19 March 2020).

[69] See above note 10.

[70] H.R. 6439 (115th): Biometric Identification Transnational Migration Alert Program Authorization Act of 2018, 9 September 2018, https://web.archive.org/web/20190716015838/https:/www.govtrack.us/congress/bills/115/hr6439/summary (accessed 19 March 2020).

and provide maintenance to the LeadTrac database, which is owned by ICE's Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit.

The database is used by units within ICE to "vet and manage leads" involving visa and immigration violations.[71] LeadTrac lets agents "query a variety of [US Department of Homeland Security (DHS)] DHS and non-DHS information systems for information on subjects" and "enter their findings into LeadTrac to build a lead – a unified picture of a subject's criminal and immigration-related activities".[72]

LeadTrac also allows agents to search a variety of other DHS databases including the Enforcement Integrated Database and the Automated Biometric Identification System.[73]

5.3. Use of private security technologies

PI has for several years been collecting information on surveillance companies and technologies within the Surveillance Industry Index (SII).[74] The SII is the world's largest publicly accessible database on the commercial surveillance sector, featuring 528 companies as of May 2016, selling a range of technologies. Any such surveillance technology can be used for identifying or tracking individuals for immigration enforcement purposes. These technologies range from targeted tools used to exfiltrate data from digital devices, to nationwide internet monitoring systems which carry out mass surveillance.

Some of the companies we have documented have been playing a role in immigration and border management including for mass data gathering and processing, communication surveillance, and location tracking, amongst others.

5.3.1 Data mining

In 2017, the Intercept reported how after winning a $41 million contract the company **Palantir** built and helped to deploy a data analysis platform – called Investigative Case Management System (ICM) – for the US Immigration and Customs Enforcement Agency (ICE). Palantir is a private American software company that specializes in big data analytics. The platform allows agents to query multiple databases at one time, as opposed to agents being required to perform the same search across dozens or more databases.[75]

The documents seen by the Intercept reveal that the ICM connects various databases managed by the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Federal Bureau of Investigation as well as other federal and private law

---

[71] US Department of Homeland Security, Privacy Impact Assessment for LeadTrac System DHS/ICE/PIA-044 22 July 2016, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leadtrac-july2016.pdf (accessed 19 March 2020).
[72] *Ibid.*
[73] See above note 45.
[74] PI, "The Global Surveillance Industry", 16 February 2018, https://privacyinternational.org/explainer/1632/global-surveillance-industry (accessed 19 March 2020).
[75] Spencer Woodman, "Palantir Provides the Engine for Donald Trump's Deportation Machine", *The Intercept*, 2 March 2017, https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/ (accessed 19 March 2020).

enforcement entities. The types of information it provides include schooling, family relationships, employment information, phone records, immigration history, foreign exchange program status, personal connections, biometric traits, criminal records, and home and work addresses.[76]

Official Department of Homeland Security (DHS) filing from June 2016 indicate that such information is not only used for deportation purposes, which is the primary task of ICE, but also for criminal and civil cases against immigrants. [77] The ICM also includes access to an internal system called the Student and Exchange Visitor Information System (SEVIS).

The Intercept also reported that Palantir developed a customised version of the company's Gotham software – which allows agents to access data from multiple US government agencies and organises it using algorithmic processing.[78] It is reported that the customised software, called FALCON, is used by ICE to access personal information such as family relationships and home addresses.

The Intercept reported that according to 2013 funding documents FALCON "will eventually give agents access to more than 4 billion 'individual data records'". Further it "gives its users the ability 'to follow target telephone activity and GPS movement on a map in real time'".[79]

5.3.2. Sale of data

Documentation PI came across showed that **Thomson Reuters Corporation** is selling access to highly sensitive and personal data to the US ICE agency, the authority responsible for implementing the US government's zero tolerance immigration policy, including the separation of families at detention centres.[80]

PI has provided federal procurement documents showing that ICE currently has contracts:

- With **West Publishing Corporation**, a Thomson Reuters subsidiary, providing it with access to the Consolidated Lead Evaluation and Reporting (CLEAR) system as part of a contract value worth over $20 million.[81] The CLEAR system[82] allows ICE access to a "vast collection of public and proprietary records" including phone records, consumer and credit bureau data, healthcare provider content, utilities data, DMV records,

[76] *ibid.*

[77] US Department of Homeland Security, Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045, 16 June 2016 https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf (accessed 19 March 2020).

[78] *ibid*.

[79] Spencer Woodman, "Palantir Enables Immigration Agents to Access Information From the CIA", *The Intercept*, 17 March 2017, https://theintercept.com/2017/03/17/palantir-enables-immigration-agents-to-access-information-from-the-cia/ (accessed 19 March 2020).

[80] PI, "Updated - Thomson Reuters Selling US Immigration and Customs Enforcement (ICE) Access to Data", 21 June 2018, https://privacyinternational.org/long-read/2079/updated-thomson-reuters-selling-us-immigration-and-customs-enforcement-ice-access (accessed 19 March 2020).

[81] https://www.documentcloud.org/documents/4546854-TR-Attachment-1.html (accessed 19 March 2020).

[82] Thomson Reuters CLEAR, The Smarter Wayto get your investigative facts straight, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf (accessed 19 March 2020).

World-Check listing, business data, data from social networks and chatrooms, and "live access to more than 7 billion license plate detections".[83]

- With **Thomson Reuters Special Services (TRSS)**, another subsidiary of Thomson Reuters, providing ICE's Detention Compliance and Removal office with "subscription data services". The contract is worth over $6.7 million and was signed in February 2018.[84] Other documentation specifies that the contract is for a "continuous monitoring and alert system to track 500,000 identities per month" which is "able to securely process and return aliens' information and addresses using the following types of specified data: FBI numbers; State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; vehicle registration information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN) data; and employer records."[85]
- With West Publishing Corporation providing its Detention Compliance and Removal office with "access to license plate reader database" as part of a contract value worth over $6 million in December 2017.[86]

PI sent an open letter to the President of Thomson Reuters Corporation asking whether he will commit to ensuring the multinational company's products or services are not used to enforce cruel, arbitrary, and disproportionate measures, including those currently being implemented by US immigration authorities.[87] The response unfortunately ignored our specific questions and made no such commitment.[88]

5.3.3. Location tracker

In February 2020, The Wall Street Journal reported that it had reviewed documentation indicating that the Trump administration had purchased access to location data, drawn from ordinary cell phone apps, including those for games, weather and e-commerce with the aim of using it for immigration and border enforcement. The documents provided information that the US Department of Homeland Security had been using this location data to identify and detect undocumented migrants and other travellers who may be entering the US unlawfully.[89]

---

83 Thomson Reuters CLEAR for law enforcement, https://legalsolutions.thomsonreuters.com/law-products/solutions/clear-investigation-software/law-enforcement (accessed 19 March 2020).

84 https://www.documentcloud.org/documents/4546855-TR-Attachment-2.html (accessed 19 March 2020).

85 Thomson Reuters to Help US Immigration and Customs Enforcement, *THE BARON*, 18 March 2018, https://www.thebaron.info/news/article/2018/03/18/thomson-reuters-to-help-us-immigration-and-customs-enforcement (accessed 19 March 2020).

86 https://www.documentcloud.org/documents/4546856-TR-Attachment-3.html (accessed 19 March 2020).

87 See above note 45.

88 See above note 80.

89 Byron Tau and Michelle Hackman, "Federal Agencies Use Cellphone Location Data for Immigration Enforcement", *The Wall Street Journal*, 7 February 2020, https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 (accessed 19 March 2020).

5.3.4. Communications surveillance

Based on documents published and made available on the US procurement records,[90] a US-based surveillance and analytics company, **JSI Telecom**, signed a contract in 2014 with ICE worth over $19.7 million for annual support, operation, and maintenance of its "Title III digital collection system".[91] The latest contract was due to end in January 2020 and it is not clear if it was renewed.

The enforcement agency intercepts wire, oral, and electronic communications—which includes the contents of calls, text messages, and emails—pursuant to judicial orders issued under Title III of the Omnibus Crime Control and Safe Street Acts of 1968 and subsequent amendments.[92] A judge can issue such an order when there is probable cause to believe that particular people committed particular felony offenses. Since 2014, federal and state authorities have submitted 14,683 applications for wiretap orders to judges, who have granted all but three of them.[93]

Other procurement records from 2017 show that Title III orders are used by ICE's investigative unit to combat "criminal organizations illegally exploiting America's travel, trade, financial and immigration systems."[94]

5.3.5. Lie detectors

The European Union's Horizon 2020 research and innovation programme has been funding a project called iBorderCtrl, defined as "an innovative project that aims to enable faster and thorough border control for third country nationals crossing the land borders of EU Member States, with technologies that adopt the future development of the Schengen Border Management.[95] In addition to other features, the system undertakes automated deception detection. [96]

The system was tested at the border in Hungary, Latvia and Greece[97]. In July 2019, The Intercept tested the system at the Serbian-Hungarian border: reportedly, the system failed

---

90 https://privacyinternational.org/sites/default/files/2019-05/FPDS-NG%20%3A%20ICDUSER%20%5B%20Award%20%5D%20jsi%20ICE.pdf (accessed 19 March 2020).

91 PI, "ICE Is Paying Millions to Surveillance Company to Spy on People's Communications", 24 May 2019, https://privacyinternational.org/news-analysis/2995/ice-paying-millions-surveillance-company-spy-peoples-communications (accessed 19 March 2020).

92 The US Department of Justice Archive, Criminal Resource Manual, CRM 1-499, CRM 1-99, Electronic Surveillance, https://www.justice.gov/jm/criminal-resource-manual-30-electronic-surveillance-title-iii-orders (accessed 19 March 2020).

93 Electronic Privacy Information Center (epic.org), Title III Wiretap Orders – Stats, https://epic.org/privacy/wiretap/stats/wiretap_stats.html (accessed 19 March 2020).

94 Federal Contract Opportunity for REQUEST FOR INFORMATION (RFI) - Title III and General Translation, Transcription, and Interpretation Services HSCEMD-17-R-00004, 20 January 2017, https://govtribe.com/opportunity/federal-contract-opportunity/request-for-information-rfi-title-iii-and-general-translation-transcription-and-interpretation-services-hscemd17r00004?__cf_chl_captcha_tk (accessed 19 March 2020).

95 iborderCtrl website, https://www.iborderctrl.eu/The-project (accessed 19 March 2020).

96 iborderCtrl Participants, https://www.iborderctrl.eu/#Project-Participants (accessed 19 March 2020).

97 iborderCtrl Pilot Results, https://www.iborderctrl.eu/Pilot-Results (accessed 19 March 2020).

and the results were not disclosed. The Intercept obtained a copy of their reporter's test only after filing a data subject access request under European data protection laws. [98]

6. Procurement rules, contractual requirements, monitoring and oversight of contractual clauses and standards, and accountability mechanisms put into place

The lack of transparency regarding the involvement of PMSCs in immigration and border management means that access to the contracts and accountability clauses are making it impossible for people to hold these companies accountable.

6.1. Regulation of public-private partnerships

Some of the main concerns relate to the lack of information as to what due diligence is in place for the decision-making related to public-private partnerships. In particular, governments should carefully consider the following prior to partnering with companies including: the ownership of the company; their business models, and how their work with governments is that firewalled from their business and commercial interests; what legal and regulatory regimes are they subject to, i.e. where are they headquartered, do they work through intermediaries; have them directly or indirectly engage in undermining human rights; have they experienced any security concerns, i.e. leaks, breaches, or other vulnerabilities.

Because of the nature of the sector they normally engage in, i.e. security sector reform, intelligence, etc., many of PMSCs don't know the specific sector in which this is deployed. This lack of understanding of the companies on the potential impact of their business models and modes of operations. Do they grasp the particular threat model of affected persons/beneficiaries as users of their services, and can they customise their products and services to mitigate the risks and threats? Are they able to clearly delineate their work within the migration sector with their commercial interests/goals?

We are also concerned by the dependency model created by such partnerships. Once a governments starts using a particular model, infrastructure or service designed and/or managed by a third party, what control do they have over the systems themselves (to modify, update, fix vulnerabilities, etc) and to what extent to they become depended on the technical expertise of the private partner indefinitely? In many cases, the company supplies, builds, operates and maintains the system they deployed, with public authorities not having sufficient knowledge or effectively overseeing the operations.

In addition to the lack of clarity with regards to the legal framework regulating such public-private partnerships, there are concerns about the enforcement of safeguards, if there are any, provided for in contracts as a result of limited or no resources to follow-up on compliance and enforcement of contractual clauses. This means that unless something goes wrong

[98] Ryan Gallagher and Ludovica Jona, "We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive", *The Intercept*, 26 July 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector (accessed 19 March 2020).

and/or is brought to their attention, public authorities may not necessarily proactively check compliance with contracts, i.e. data was not shared with other parts of the company, not contribute to inform business model, or that they delete the data they may have been handed over/processed after the programme is over. With this in mind, it is not enough for such risks and threats and concerns to be solely managed and regulated through contracts. There must be more to the assurances companies provide so governments can effectively oversee their implementation and guarantee they are taking measures to protect migrants.

Companies are driven by the generation of profit, and accountable to Board and their shareholders. Some companies/industry are founded - and dependent - on a data exploitative model which fails to meet any sort of human right protection and/or concern itself with protecting people affected by the systems and infrastructure they build. Apart from generating profits, it is clear that their priorities are not focused on protecting people.

6.2. Lack of transparency and oversight of funding

One key area which PI has been exploring in relations to the role of industry in immigration and border management has been the transparency and oversight of funding enabling these public-private partnerships. It is often public funds that drive the expansion of an industry to a specific sector and nowhere is this clearer at the moment than in the migration sector. Where at the moment, countries with the largest defence and security sectors, such as the EU, encourage and enable other governments to deploy advanced surveillance capabilities without adequate safeguards to counter-migratory movements. This ties into what was referred above as border externalisation and border digitalisation.

Exemplary of this trend is the EU diversion of aid funds agreed in 2015. The EU Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa (EUTF for Africa) uses development aid and cooperation funds to manage and deter migration to Europe. It currently funds numerous projects presenting urgent threats to privacy, including developing biometric databases, training security units in surveillance, and equipping them with surveillance equipment.[99]

The main forms in which such provision come in include direct equipping of equipment of foreign intelligence and security forces, training of foreign intelligence and security forces, the financing of their operations and procurement, the facilitation of exports of surveillance equipment by industry and the promotion of legislation which enables surveillance. There must be greater transparency of such assistance to other governments. There needs to be an end to the transfer of unlawful surveillance, and for the promotion transfer of adequate privacy protections.[100]

[99] Resources currently allocated to the EU Trust Fund for Africa as of July 2019 amount to EUR 4.6 billion including more than EUR 4.0 billion from the European Development Fund(EDF),the EU's main instrument for development aid, the Development Cooperation Instrument(DCI), and the European Neighbourhood Instrument(ENI),funding from the Directorate General (DG) for Migration and Home Affairs and DG European Civil Protection and Humanitarian Aid Operations(ECHO). EU Member States and Norway and Switzerland have so far contributed EUR 526 million. See above note 12.

[100] See above note 2.

The EU Funds have been used to fund national centralised biometric databases in various countries in Africa (Senegal and Côte d'Ivoire among others)[101], as well as surveillance equipment, such as international mobile subscriber identity catchers (IMSI catchers)[102] and wiretapping equipment for border agencies in Niger. They also fund training on using surveillance technologies for authorities across Africa.[103]

Besides supporting operations by border security forces, European donors funded also data collection systems. The Migrant Information and Data Analysis System, a migration database partially funded by the EU and installed at land borders, might interact in the near future with the West Africa Police Information System, a criminal database funded by Brussels to gather and share biometric information in 17 countries in West Africa. Frontex, the EU border guard agency, will be able to analyse a part of this information.

These processes are sanctioned without the levels of transparency and oversight required. The EU Trust Fund for Africa has been put together hastily without due diligence procedures in place or consideration of the impact of these policies. The European Court of Auditors has found that, while it is a flexible tool for providing assistance, its objectives are too broad, and the Commission has failed to appropriately measure the extent to which it has met its objectives. Further, the Fund lacks key transparency and oversight mechanisms because the European Parliament is only currently an "observer". The significant privacy and data protection concerns present a major threat to people's human rights, security, and to democratisation in third countries.[104]

In the meantime, the companies procuring the contracts funded under such schemes, such as Civipol, Palantir and thousands of others, are left unsupervised to implement the projects as it best suits their business plans. Their priorities do not include the protection of the rights of migrants. This is driven and sanctioned by these public funds that are distributed and spent with no transparency or oversight throughout the process.

PI has tried repeatedly to obtain access to documentation about these contracts, but these were never made public, and so it has not been possible to know what, if any, oversight and accountability measures exist.

7. The role of private security providers in shaping a security narrative around migration

The increased potential to generate more data, track people across services, and make determinations on status and eligibility, all brought by companies selling capabilities, drive government ambitions.

---

[101] See above note 12.

[102] PI, "Explainer – IMSI Catcher", https://privacyinternational.org/explainer/2222/imsi-catchers (accessed 19 March 2020).

[103] PI, "The EU Funds Surveillance Around the World: Here's What Must Be Done About It", 18 September 2019, https://privacyinternational.org/long-read/3221/eu-funds-surveillance-around-world-heres-what-must-be-done-about-it (accessed 19 March 2020).

[104] European Court of Auditors, EU trust fund for Africa: flexible emergency tool, but lacking focus, 5 December 2018, https://www.eca.europa.eu/en/Pages/NewsItem.aspx?nid=11356 (accessed 19 March 2020).

Companies are fulfilling a demand from governments for tech-driven and data-intensive migrations systems they want to deploy. The increase in demand for such systems means that they have an increasing demand for their solutions which is driving their profits.

Over the years, we have seen private security providers marketing themselves as the providers of solutions for governments to tackle the most pressing challenges from the delivery of public services to law enforcement as well as immigration enforcement. The marketing brochures collected by PI over the year from surveillance companies and technologies as presented in the Surveillance Industry Index (SII) show the evolution [105]

A report by the Transnational Institute (TNI) calls out the development of the 'EU Security-Industrial Complex' and argues that the legislation for the €1.7 billion security research programme within Horizon 2020, the EU's 2014-20 research and technological development programme, could have taken a very different turn had it not been amended to a more "industry friendly" text.[106]

Others have also argued how private military and security companies "frame, shape and entrench militarized responses in the European Agenda."[107] The article outlines through the presentation of evidence from contracts between the European Asylum Support Office (EASO) and various private military and security companies from 2017: *"the EU and its Member States to respond to the refugee 'crisis' have increasingly enabled the outsourcing to PMSCs of various migration control operations, including inter alia those related to deportations and removal, housing, transport, the detention of refugees and the security of reception and/or processing centres, such as the 'hots pots' in Italy and Greece*."[108]

Similar concerns were raised by other organisations. Statewatch and Belgian NGO "Vredesactie" conducted research which showed how successful European military and security industry have been in shaping and influencing EU military and security policies.[109] They reported the extensive lobbying activities of large European arms companies, including as **Airbus** (Pan-European), **Leonardo** (Italian, formerly called Finmeccanica) and **Thales** (French) through their lobby associations, which include the European Organisation for Security (EOS) and the AeroSpace and Defence Industries Association of Europe (ASD), were able to put pressure and gain influence as evidenced by how some of their proposals were in some instances adopted directly by European bodies. These companies have been involved in supporting immigration and border management policies and practices including donations of patrol boats from shipbuilder **Intermarine** to Libya, or the purchase of vessels for Turkey to strengthen the capacities of its coast guard.

---

[105] See above note 73.

[106] Statewatch and tni, "Market Forces: The development of the EU Security-Industrial Complex", https://www.tni.org/files/publication-downloads/marketforces-report-tni-statewatch.pdf, p. 36.

[107] Daria Davitti, "The Rise of Private Military and Security Companies in European Union Migration Policies: Implications under the UNGPs", (2019) 4(1) *Business and Human Rights Journal* 33, https://doi.org/10.1017/bhj.2018.21 (accessed 19 March 2020).

[108] *ibid*., p 34.

[109] Transnational Institute, "How the Security Industry Reaps the Rewards of E.U. Migration Control", 5 June 2018, https://www.tni.org/en/article/how-the-security-industry-reaps-the-rewards-of-eu-migration-control (accessed 19 March 2020).

Another example reported by is that **Civipo**l, technical cooperation operator of the French Ministry of the Interior which is part-owned by large arms producers as Thales, Airbus and Safran, wrote "an influential consultancy paper" called "*Feasibility study on the control of the European Union's maritime borders"* for the European Commission, that went on to provide the foundations for then became the current measures and policies on border externalisation.[110] Over the years, Civipol has been involved in various border management projects including organising formation of a border guards in Morocco, purchase of material and equipment for land and sea border surveillance units in Tunisia, setting up fingerprint databases of the whole population of Mali and Senegal, amongst other projects.[111]

8. Allegations of human rights abuses against migrants

Privacy is a human right and any form of surveillance which is unlawful, not necessary and disproportionate, not subject to adequate safeguards, is itself a human rights violation. But privacy is also an enabling right on which the enjoyment and protection of other rights depends. Interference with our privacy often provides the gateway to the violation of the rest of our rights, even more so of migrants that are found in vulnerable positions.

The deployment of operation of the above technologies by PMSCs and public authorities risks leading to serious violations of the right to privacy of millions of migrants across the globe to the detriment of the exercise of their other rights as well. First, where there is often no legal framework regulating the deployment of these technologies, their use in unlawful. Second, the interference with privacy is not necessary to achieve the purpose for which they are deployed, and they constitute a disproportionate interference with the privacy of people that are stripped of their autonomy and dignity. Third, in most cases there are not sufficient safeguards to protect the migrants against undue interferences with their privacy. There is no effective oversight and there are no effective remedies.

More often than not these abuses of privacy go unreported because of the vulnerable position in which migrants are found. They need shelter and aid not only for themselves and their loved ones. They need work and a home. They often don't speak the language. Protecting their privacy is not an option, but in the process the loose their autonomy and dignity.

For people at risk, privacy is essential. Privacy, when properly respected should prevent states with poor human rights records and other malicious actors from monitoring individuals' communications in a way that undermines their rights and dignity.

There have been numerous reports documenting the scope and nature of the human rights abuses, particularly when it comes to the EU migration control policies.[112] Leading organisations such Human Rights Watch have documented human rights abuses against migrants including as a result of "restrictive entry, screening, and immigration detention

[110] See above note 56.
[111] See above note 56, pp 78-79
[112] Davitti, note 107, pp.35

policies that expose migrants to abuse, extortion, and violence at border crossings", [113] with others reporting on how the increased privatisation of border management and refugee services is leading to increased death and health issue[114].

However, the role of interference with their privacy in the process is often overlooked. Some surveillance technology is traceable because it leaves a digital signature on a targeted device or because its operation can be mapped through technical analysis. For example, the Citizen Lab has been able to use such techniques to map the use of surveillance technology targeted at human rights defenders and others.[115]

However, other types of surveillance technology do not leave any traceable signatures: for example, if an immigration agency were using a mass internet surveillance tool to track people's communications, tracing the interference with privacy to the subsequent torture of an individual would be difficult without, for example, testimony from someone involved in the surveillance process itself.

The lack of transparency and oversight in these processes makes it difficult to understand how other human rights abuses, such as torture, are facilitated by surveillance technology provided or operated by a private company. This would require documenting a connection between the use of that technology by an agency implicated in such abuses. This is incredibly difficult given secrecy provisions surrounding how immigration agencies use surveillance technology: even within relatively established democracies, agencies are not open about how they use such technology.

In 2007, French technology firm Amesys (a subsidiary of Bull) supplied sophisticated communications surveillance systems to the Libyan intelligence services. The systems allegedly permitted the interception of all country-wide, on-line and phone communications and the subsequent processing of collected data.[116]

There are numerous reports on extrajudicial killings in Kenya where the individuals were last seen with Kenyan security officers. What is less reported is how these operations have been facilitated by communications surveillance. In 2017, PI revealed how intelligence gained by

---

[113] HRW, "Rights on the Line, Human Rights Watch Work on Abuses against Migrants in 2010", 11 December 2010, https://www.hrw.org/report/2010/12/11/rights-line/human-rights-watch-work-abuses-against-migrants-2010 (accessed 19 March 2020).

[114] Jane Lethbridge, "Privatisation of Migration & Refugee Services & Other Forms of State Disengagement", Public Services International and European Public Service Union, March 2017 https://www.epsu.org/sites/default/files/article/files/PSI-EPSU%20Privatisation%20of%20Migration%20%26%20Refugee%20Services_EN.pdf (accessed 19 March 2020).

[115] TheCitizenLab, "NSO Group / Q Cyber Technologies Over One Hundred New Abuse Cases", 29 October 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/ (accessed 19 March 2020).

[116] Under the Regime of Muammar Gaddafi, the technology became a weapon that facilitated the targeting, arrest and imprisonment of thousands of people in Libya. In 2011 the International Federation for Human Rights (FIDH) and la Ligue des droits de l' homme (LDH) brought a criminal case against Amesys for complicity with human rights abuses committed by the Gaddafi regime in Libya because they provided to it surveillance equipment. In 2018, Theresa May publicly issued an unprecedented apology for Britain's role in the kidnap and torture of Libyan dissident Abdel Hakim Belhaj and his wife, Fatima Boudchar by the Gaddafi regime. UK's Secret Intelligence Service (MI6) shared intelligence with the CIA and Libya's External Security Agency, leading to their abduction. Fidh and Ligues des droits de l'homme, The Amesys case, 2014, https://www.fidh.org/IMG/pdf/report_amesys_case_eng.pdf (accessed 19 March 2020); PI, "Privacy matters because…it can protect us from torture", https://privacyinternational.org/case-study/3319/it-can-protect-us-torture (accessed 19 March 2020).

intercepting phone communications.[117] These are not necessarily examples related to migrants, but they graphically illustrate the connections between the surveillance and data exploitation practices to manage and deter migration.

Conclusion

As outlined in our submission, PMSCs are playing a central role in in immigration and border management in the form of the provision and operation of surveillance technologies and data exploitation processes, as well as other services.

Government and public authorities responsible for immigration must stop using unlawful techniques for immigration control and they must be transparent about the new ways in which technologies and private companies are being used to make decisions about migrants, including through the expansion of databases, watchlists, and the types of data collected.

Companies must stop supplying and operate invasive techniques to implement immigration policies that are discriminatory and curtail the rights of migrants. There must be transparent procurement and due diligence processes to ensure that the solutions they are providing to governments are not used to violate the rights of migrants.

The above situation is having a huge impact on migrants through surveillance and data-driven immigration policies leading to discriminatory treatment of people and undermining peoples' dignity. These practices mean that migrants are bearing the burden of the new systems and losing agency in their migration experience, particularly when their fate is being put in the hands of systems driven by data processing and tech innovation.

There is a need to demand a more humane approach to immigration based on the principles of fairness, accessibility, and respect for human rights.

PI appreciates the intention of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination to shed more light on the role of private military and security companies in immigration and border management and the impact on the protection of the rights of all migrants. We are looking forward continuing to engage with the Working Group on this and other processes to ensure we are all free to be human.

[117] PI, "Privacy matters because…it can protect our lives, https://privacyinternational.org/case-study/3316/it-can-protect-our-lives (accessed 19 March 2020).

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321

privacyinternational.org