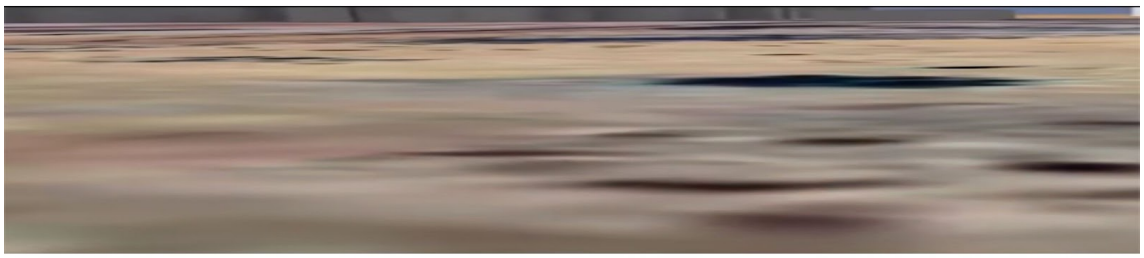
CYBERSECURITY IN SURVEILLANCE AND BORDER CONTROL

OPRESSIVE CYBER THREATS FOR IMMIGRATION



data mining geo tagging biometric processing

Elisa Schmitz, Ciro Longobardi, Francisco Pérez

Table of Contents

Introduction

Europe has a history of welcoming refugees. The 1951 Refugee Convection was established in response to the urgent needs of refugees arising from the Second World War. Since then, Europe has welcome asylum seekers fleeing conflict, persecution, and violation of human rights. The number of refugees in the European region fluctuates increasing in times of instability and calming down as solutions are found for them.

This constant flow of people seeking asylum in Europe for many circumstances has affected the governments of many EU members countries which have decided to use the technology on behalf of the control of their frontiers, making the situation more difficult for these refugees and in some cases violating all kinds of privacy rights.

To help getting into context we are going to give you some data that will hopefully arise some knowledge of how technology can be used in certain in these cases.

In 2021 Polish government invested €350M in advance military technology to police its borders with Belarus, this equipment includes drones, cameras and sensors, surveillance centers intercepting communications and IA technology for biometrical and face recognition.

This is not an isolated case, in 2020 the EU predicted the European Security Market to grow in €128bn, beneficiaries are arms and tech companies who are selling their equipment to EU countries for frontier control.

This kind of equipment has low or inexistence regulation, as IA and drone surveillance is brand new, therefore the use of them in most cases is inappropriate vulnerating privacy, and the United Nations charter.

Air Surveillance

The most expensive tool is the long-endurance Heron drone operating over the Mediterranean.

Sensors and cameras

EU air assets are accompanied on the ground by sensors and specialized cameras that border authorities throughout Europe use to spot movement and find people in hiding. They include mobile radars and thermal cameras mounted on vehicles, as well as heartbeat detectors and CO2 monitors used to detect signs of people concealed inside vehicles.

Artificial intelligence

A machine scans refugees and migrants' facial expressions as they answer questions it poses, deciding whether they have lied and passing the information on to a border officer, this is based on a large database of human expressions constructed using data mining techniques and biometrical processed information.

The software is the subject of a court case taken by MEP Patrick Breyer to the European court of justice in Luxembourg, arguing that there should be more public scrutiny of such technology.

This is and underline of the current situation in Europe and there are many different technologies used in frontier control a surveillance, to relate to our main research topic on Cybersecurity we are going to make emphasis and focus on 3 main techniques used:

Data Mining

By associating rules data patterns become more intelligent and can identify specific activities.

Immigration and Customs enforcement agents work together with companies that analyze massive amounts of data. In this way agents can prosecute undocumented immigrants. Data Mining then works as a core law enforcement case management tool.

Geotagging

The Geo tagging feature is, an awesome way of letting people know where you had that delightful lunch with your family, or the beautiful view from your room during a holiday trip. It just makes it easier for you to arrange photos and let friends know where they might be able to replicate some enjoyable experience you had.

With its interesting capabilities, there is also risk considering when using the Geo tag feature, especially when this feature can be used to track vulnerable people in the border control and control their movements.

Biometric Processing

Biometrics refers to the automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits, and odors.

Biometrics technology is well known and facilitates many processes of identification and authentication but used with the wrong purpose it can become a real method of control, surveillance and track of refugees crossing the borders.

So is this, that there has been a leak of the European Union using biometric technology not only for identifying, but for sharing this data and matching the country from which immigrants come from, so that they can easily return them if necessary. This data is not securely shared and currently violates the actual European Data Protection Act.

The major concerns on the use of this technology are:

- **Biometric technology is inherently individuating and interfaces easily to database technology**, making privacy violations easier and more damaging.
- **Biometrics are no substitute for quality data about potential risks,** they must not be used solely to target if a person is a security risk to the country or not.
- **Biometric identification is only as good as the initial ID,** it means that it just works once there has been a previous enrollment or registration which involves data sharing, if initial ID is fake and associated to real biometrics, this will be a way to bypass the system.
- **Biometric identification is often overkill for the task at hand**, it is not necessary to identify a person (and to create a record of their presence at a certain place and time) if all you really want to know is whether they're entitled to do something or be somewhere. When in a bar, customers use IDs to prove they're old enough to drink, not to prove who they are, or to create a record of their presence.
- **Some biometric technologies are discriminatory**, there are certain people that cannot present suitable features to participate in certain biometric systems, for example those with bad fingerprints.
- **Biometric systems accuracy is impossible to assess before deployment**: Accuracy and error rates published by biometric technology vendors are not trustworthy, as biometric error rates are intrinsically manipulable. Biometric systems fail in two ways: false match (incorrectly matching a subject with someone else's reference sample) and false non-match (failing to match a subject with her own reference sample). There's a trade-off between these two types of error, and biometric systems may be "tuned" to favor one error type over another. When subjected to real-world testing in the proposed operating environment, biometric systems frequently fall short of the performance promised by vendors.

- **The cost of failure is high.** If you lose a credit card, you can cancel it and get a new one. If you lose a biometric, you've lost it for life. Any biometric system must be built to the highest levels of data security, including transmission that prevents interception, storage that prevents theft, and system-wide architecture to prevent both intrusion and compromise by corrupt or deceitful agents within the organization.

In the case of refugees this technology is used by organizations such as Frontex (European Border Control) as surveillance equipment. By far the most significant negative aspect of biometric ID systems is their potential to locate and track people physically. While many surveillance systems seek to locate and track, biometric systems present the greatest danger precisely because they promise extremely high accuracy.

Whether a specific biometric system poses a risk of such tracking depends on how it is designed.

This is just a small glimpse on the kind of technology used, and the well-known situation in Europe in relation to refugees to introduce you, the reader into a subject that is going unnoticed and to analyze more in depth how countries are using cybertechnology in surveillance and border control, the impact on the people subjected to it, how help and support groups are fighting against these privacy violations and some ways in which these control can be mitigated.

The relationship between tech companies and governments in the surveillance and control of their borders.

Contemporary border control and migration management policies and practices of the European Union are structured within a framework characterized by an intimate collaboration between public and private interests, with public interests broadly represented by EU agencies and member states, and private interests by security and defense companies, lobbying consultancies, law firms, universities, and research institutes.

Particularly defining about the public-private collaboration is the increased reliance on advanced and innovative border technologies which are developed and deployed with the dual aim of controlling irregular migration, and simultaneously, sealing off and securing the European borders. These advanced and innovative border technologies range from pre-screening technologies like biometrics comprising of facial features and fingerprints, to land and maritime surveillance by technologically advanced systems like early warning radar systems and unmanned aerial vehicles (UAVs) that can detect suspicious movements or vessels from a certain distance. This has created a market for technologically advanced software, technologies and equipment that is shaped, supported, and provided primarily by major security and defense companies such as Airbus (formerly known as EADS and henceforth Airbus/EADS), Finmeccanica (now known as Leonardo), Thales, BAE Systems, and Safran, in collaboration with software companies, universities, research centers and think-tanks making migration control a profitable and viable option.

With the increase of terrorism in the past decade and this having turned to an increase in the number of immigrants to European countries, there is a conflation of security with migration and border control. Consequentially, this transforms into and ascent of security and defense companies with public entities. In the aftermath of the terrorist attacks of 9/11 on 11th September 2001, the Madrid Bombings on 11th March 2004, and the London Bombings of 2005, we witness a robust involvement of security and defence companies allegedly providing ‘security’ through a range of technological innovations. The deployment of advanced technologies simultaneously fulfils the role of fortification and securitization centered on the figure of the migrant.

The European Union (EU) security market has a global market share of 25-35 %, ranking second to the US security market which is the market leader (ECORYS 2009). The EU security market is estimated to have an annual turnover of €30 billion, employing around 180,000 persons (European Commission 2016, ECORYS 2009, European Commission 2012: 10). The global security market is dominated notably by Lockheed Martin, Boeing, Raytheon, Northrop Grumman and United Technologies, capturing a 40 % market share (ECORYS 2009, Gloannec et al. 2013, Relyea 2002, SIPRI 2016).

The various market segments of aviation, maritime, border security and counter-terror intelligence are used to intersperse and punctuate a migrant's journey with a range of border technologies. These border technologies comprise of information communication technologies (ICTs), smart walls and fences enabled with sensors and cameras, biometrics based on facial features, iris and fingerprints, stationary and mobile surveillance systems equipped with technologically advanced systems like early warning radar systems, unmanned aerial vehicles (UAVs) and drones which are deployed for identification, surveillance, detection, and interception. The key segments that perceptibly caters to migration and border control along the migration security linkage are primarily aviation, maritime, border security and counter-terror intelligence as they comprise of technologies that install controls and barriers to detect, identify, intercept, track, and trace migrants. This reflects a technological labyrinthine that interrupts a migrant's journey at every point with the aim to prevent his/her arrival, to detect, intercept, surveil, track and return (Bigo 2013, Carrera et al. 2008, Pickering and Weber 2006).

Here we can see a brief description of what this market segments do:

- Aviation or air security refers to the "detection, identification, tracking and tracing of goods and persons for secure and safe air transport" (ECORYS 2009: 91). This sector has "grown considerably in the aftermath of 9/11" (ECORYS 2009: 91) owing to the nature of the attacks whereby a scanned and screened airplane was used as a weapon to conduct the attacks.

- Maritime or sea security refers to the "detection, identification, tracking and tracing of goods and persons for secure and safe maritime transport" (ECORYS 2009: 133). The sector includes "sea safety and security, sea environment, fisheries, trade and economic interests of the European Union as well as the general law enforcement and defense" (Sempere 2011: 65). Like the aviation sector, this sector has witnessed growth due to concerns of a "9/11 type of a terrorist attack that can happen at the seas or a port by using a ship as a terrorist weapon" (ECORYS 2009: 52).

- Border security refers to the "controlling of border checkpoints and the surveillance of unregulated frontiers deployed with the aim of restricting 'illegal' immigration, terrorism, and organized crime" (Sempere 2011: 64).

- Counter-terror intelligence is one of the “fastest growing market segments along with the aviation sector” (ECORYS 2009: 32). This segment caters to “high level security threats which is high on the political agenda” (ibid.). It involves the “gathering of information, monitoring, detection, maintaining profiles and databases, analysis of databases and communication” (Sempere 2011: 4) and as a market segment, it overlaps with other market segments, particularly due to its concerns to pre-empt the next terrorist attacks.

Some of this companies collaborating are:

Border Technologies	**Key Companies**
Aircrafts/Drones (Civil and military aircrafts)	Airbus, Aérospatiale, BAE Systems, Boeing, Dassault, Diehl, Finmeccanica, Lockheed Martin, Northrop Grumman Corporation, Safran Group, Thales
Biometrics	Accenture, Cogent Systems, Image Ware Systems, Indra, Iris Guard, L-1 Identity Solutions, Motorola, NEC Advanced Security Solutions, Lockheed Martin, Northrop Grumman, Precise Biometrics, SAGEM Morpho, Sagem Sécurité, Unisys
Command and control systems Port Access Control	BAE Systems, Airbus/EADS, Indra, Kongsberg, Thales
Communication systems	Atos Origin, BT Global Services, Cap Gemini, Cisco, Deutsche Telekom (T-Systems) IBM, Airbus/EADS, Motorola, Harris Corporation, Selex, Telefónica, Telecom Italia
Perimeter security systems	Alenia Aeronautica, BAE Systems, Dassault, Airbus/EADS, EMT, Indra, Kongsberg, Meteor, Saab, Sagem, Thales
Radiofrequency identification (RFID)	Avery Dennison, Checkpoint Systems Inc., Datamars SA, HID Global, IBM, Intel, Infineon Technologies, Intermec Technologies Corp., Philips Semiconductors, Savi Networks, Sensormatic –Tyco, Sokymat, ST Microelectronics, Sun Microsystems, Tagmaster/ WaveTrend, Texas Instruments Radio Frequency Identification Systems, UPM Raflatac
Screening and scanning	Bruker Daltonics, General Electric, Gilardoni, L-3 Communications Corporation, Rapiscan Systems, Smiths Detection
Surveillance, tracking and tracing	Axis Communication, Bosch Security Systems, Cassidian, G4S Securitas Group, Gunnebo, Honeywell, Ingersoll -Rand

Some cybersecurity related measures to protect refugee’s privacy

As a matter of concern and as refugees have not got many ways to protect against this issue, we have made in-depth research of some personal measures that migrants can take when crossing the border.

First, take into consideration that agents are not going to be worried about your privacy or security of your information, so you must be aware that it is going to be (unfortunately) your sole responsibility.

Encryption is your main ally, so you must use passwords across all your devices and be aware that although we may think that digital fingerprints are more secure, they are not a recommendation when crossing borders as agents may simply force you to unlock your device. It is also recommended to encrypt your entire device and switch it off when crossing the border.

When finishing the process of crossing the border, change all your passwords and establish new secure ones, you can use a password manager to help you on this task.

Data store in the cloud are more protected than the ones store in your devices, this means that you should make backups of your information to the cloud and delete them from your devices, you can the retrieve it once you close the border.

This are some recommendations given to protect when crossing the border, although we may arise the fact, that unfortunately your personal information been secured is never guaranteed.

Empowering refugees with technology

When focusing on the research we found a company focused mainly on giving for free technology skills and security advised to displaced persons, supporting them, and making them more aware of cyber threats and data protection.

An example of it is Techfugees an international organization mobilizing a community of developers, humanitarians and social entrepreneurs creating sustainable digital solutions contributing to the inclusion of displaced people.

Techfugees supports the reconquest of the autonomy of displaced people through digital innovations made with, for and by them.

Some of the principles and recommendations by which Techfugees rules:

Displaced persons can be helped as well as harmed by the use of data.

Protecting these vulnerable people from the harms posed by data use is a shared responsibility.

Here a few recommendations to bear in mind:

- *The collection, generation and use of data should never be done simply because they can be the need and potential benefits should be clear, defined and justified to respond to a need or improve the service towards refugees.*
- *Presume that all your users will not read the terms and conditions of your technology product. Consider the ethical implications of collecting data when building your product.*
- *If you choose to disclose data, it must not lead to already vulnerable individuals and communities being further harmed or exploited. In case where it is possible, pre-identify risks associated with a proposed used of data. – Assume that hostile regimes may attempt to access data for the wrong reasons. Most State*

supported hackers and some Government surveillance services are capable of hacking any data.

- *As most data breaches and leaking come from human failure, it matters that you take extra care in the way you store, who has access and how one can get access to the data. Make sure to always adhere to legal and ethical standards in place.*
- *Any data or results deriving from a population should be shared with that population. Too many communities in tech projects get asked for their data without seeing the results!*
- *Overall, this data responsibility rule goes beyond the concepts of "data privacy" and "data protection". It entails a set of principles, processes and tools that seek to leverage data to improve people's lives in a responsible manner.*

Conclusion

As a summary of our research, we must arise three facts of the issue that has been approached.

Surveillance and border control is a reality, and refugees rights are being violated when crossing to other countries seeking safety and asylum.

Technology has been used for this task and security of the data been collected is not taken into consideration. In the same way big tech companies are developing cyber weapons for control and making profit from it.

Cybersecurity is a matter that should be concern, to regulate and protect the data been collected and for refuges not to be exposed to this cyber threat from oppressive governments.

Therefore, with this research paper, we pretend to make the reader aware of the situation and to help those in needs with the resources and documentation on cyber threats that may arise when crossing borders and how they can be protected.

Bibliography

(s.f.). Obtenido de https://www.webroot.com/us/en/resources/tips-articles/tag-youre-it-are-geolocation-services-making-a-cybercase-out-of-you

(s.f.). Obtenido de https://www.cybersecurity-review.com/tag/geotagging/

(s.f.). Obtenido de https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/using-technology-to-prevent-and-combat-tip-and-som.html

(s.f.). Obtenido de https://www.nbcnews.com/news/us-news/gps-tracking-immigrants-ice-raids-troubles-advocates-n1042846

(s.f.). Obtenido de https://privacyinternational.org/explainer/4796/electronic-monitoring-using-gps-tags-tech-primer

European Parliment. (s.f.). Obtenido de https://www.europarl.europa.eu/news/es/headlines/society/20170627STO78419/los-controles-fronterizos-de-la-ue-y-la-gestion-de-la-migracion

Foundation, E. F. (s.f.). *Electronic Frontier Foundation*. Obtenido de Biometrics: Who's Watching You?: https://www.eff.org/es/wp/biometrics-whos-watching-you

IBM. (s.f.). *IBM*. Obtenido de https://www.ibm.com/cloud/learn/data-mining

International Comitee of the Red Cross. (s.f.). Obtenido de https://www.icrc.org/en/document/cyber-security-how-it-affect-me

Karspersky. (s.f.). Obtenido de https://latam.kaspersky.com/blog/digital-searches-at-border/12361/

Migration Media. (s.f.). Obtenido de https://migrantmedia.network/wp-content/uploads/2021/04/MMN_game_ghana_poster_2020_for_internet_use-2.pdf

Press, A. (16 de 11 de 2021). *Voanews*. Obtenido de https://www.voanews.com/a/poland-uses-water-cannons-against-migrants-at-belarus-border-/6315956.html

Security Info Watch. (s.f.). Obtenido de http://www.securityinfowatch.com/

Techfugees. (s.f.). Obtenido de https://techfugees.com/techfugees-guiding-principles/

The Bureau Investigates. (s.f.). Obtenido de https://www.thebureauinvestigates.com/stories/2020-04-28/monitoring-being-pitched-to-fight-covid-19-was-first-tested-on-refugees

The new Humanitarian. (s.f.). Obtenido de https://www.thenewhumanitarian.org/news-feature/2019/06/06/biometrics-new-frontier-eu-migration-policy-niger

The Risk of Geotagging. (s.f.). Obtenido de https://safeonline.ng/social-media/understanding-the-risks-in-geo-tagging/

The role of security and defence companies in EU migration and border control and the impact on the protection of the rights of refugees, m. a. (s.f.). Obtenido de https://www.ohchr.org/Documents/Issues/Mercenaries/WG/ImmigrationAndBorder/kumar-submission.pdf

Tondo, K. A. (s.f.). *The Guardian*. Obtenido de https://www.theguardian.com/global-development/2021/dec/06/fortress-europe-the-millions-spent-on-military-grade-tech-to-deter-refugees