Smart Borders, Digital Identity and Big Data — Chapter Notes

Nov 4, 2026 · @Emre Eren Korkmaz

The book at a glance

Core thesis. Migration management, border security and humanitarian emergencies are where technology, military and financial corporations test and develop new surveillance technologies. If those pilots succeed and meet no resistance, the same tools spread to the rest of society. Migrants are "the canaries in the coal mine" (Ruben Andersson, 2022).

What sets the book apart. Most critical work looks at the *use-value* of surveillance technology: what clients (governments, UN agencies, NGOs) do with it and the harm that follows. This book looks at the *exchange-value*: why corporations build, test and sell these products, and why advanced capitalist states fund and buy them. The technology is treated as a means of production owned by capitalists. It is not a neutral tool.

Two lenses used together.

- *Reformist*: case studies of discrimination, errors and rights violations, with fixes such as better data, human oversight and explainability.
- *Structuralist*: how technology changes capitalism, labour relations and class positions, and the global division of labour.

The argument in four steps.

1. Surveillance capitalism is a structural feature of today's capitalism, not just the business model of a few Silicon Valley firms (Chapter 1).
2. Big data collected from migrants, through phones, social media, satellites, drones and sensors, is the raw material (Chapter 2).
3. Smart borders use that data to select "desirable" migrants and keep the rest away, ideally before they reach the border (Chapter 3).
4. Digital identity decides where, how and by whom the data is stored. It monitors and integrates those allowed in as workers (Chapter 4).

Key move. The literature treats smart borders and digital identity separately. The book joins them as two sides of capitalism's approach to migrant labour: rejecting some people, then selecting, steering and exploiting the rest.

Key concepts. Surveillance capitalism · exchange-value vs use-value · technological solutionism · the "metaphysical" view of technology as neutral · pilots, with migrants as guinea pigs · humanitarian agencies as data suppliers to Big Tech · the donor–recipient hierarchy · selecting migrant labour to raise surplus-value extraction.

Introduction: Canaries in the Coal Mine (pp. 1–15)

Argument. Technological change is a political conflict over "what is the world that we want to live in?" Political and social problems need political solutions. Technology alone tends to reinforce existing

inequalities. Migration and border management are where surveillance products are piloted first, so they show where capitalism is heading.

Key points

- **Technology as a means of production.** An algorithm, robot or drone has no intention of its own. It answers to the capitalists who own it, decide what gets produced and extract value from it. So the analysis should focus on owners and their interests, not on "what AI does".
- **Exchange-value vs use-value.** NGO and academic critiques (e.g. Privacy International) target clients and the use-value of surveillance tech. The book asks why tech, military and financial firms build and test it, with advanced capitalist states acting as funders and clients.
- **Reformist vs structuralist approaches.**
    - Reformist: algorithmic bias in US policing and sentencing (O'Neil, Noble), the 2021 UK exam-grading algorithm, gender bias in translation ("O doktordur" becomes "He is a doctor", "O hemşiredir" becomes "She is a nurse"), human oversight of autonomous weapons, gig-worker campaigns. Fixes include better data, participatory design and explainability.
    - Structuralist: precarious work, inter-state competition, unemployment, monopoly, (neo)colonialism and dependency (Fuchs, 2019).
    - The book uses both.
- **The "metaphysical" view of technology** (Joque, 2022). Treating algorithms as objective, neutral and scientific hides the power and ownership behind them.
    - A visa or asylum refusal by an algorithm is accepted more readily than one by a consul or border agent.
    - The UK grading case: the government blamed the algorithm and cancelled the markdowns, so the deeper class divide between state and private schools never became the issue.
    - Prediction is just the most probable option. "80% risk" still leaves 20%. That is fine in chess or Go, but not for asylum decisions, where the 20% may face death.
    - AI lie-detector kiosks at borders (sensors read gestures, perspiration, skin colour and anxiety). Even a claimed 70% success rate leaves 30% wrong.
    - People who would protest a racist border agent go quiet when the process is automated.
- **Virtual walls vs physical walls.** US Democrats opposed Trump's wall but both parties back the "virtual wall" of sensors, fake phone towers and drones. It is more socially acceptable but pushes migrants onto deadlier routes and causes more deaths (Franco, 2019; Mijente, 2019).
- **The tools spread beyond migration.** If border lie detectors meet no opposition, expect them in workplaces, schools and police stations. Example: a worker doing undercover union organising confesses out of fear of the detector.

- **Migrants as guinea pigs.** Deployments are called "pilots" because the products are not finished (Molnar, 2021a). Example: the 2022 "high-tech closed refugee camps" on three Greek islands (Molnar, 2021b).
- **The link to war technology.** Border drones can be turned into weapons. Robot dogs patrol the US–Mexico border. Sensors and satellites that watch for migrants also gather intelligence on neighbouring states, which threatens regional peace.
- **A global consensus.** The US, UK, EU, Australia and Canada share the approach, as do Global South states (Turkey, Mexico, Bangladesh). A small number of tech and military firms sell to all of them.
- **Rights advocacy is necessary but not enough.** The rights already exist in law but are denied to certain categories of people. Focusing only on rights implies that changing governments would fix things.
- **Selection of migrant labour.** Migration management decides who joins the labour market, in which sectors and on what wages. Data analysis makes selection faster. UN and humanitarian agencies are becoming data suppliers to Big Tech.
- **"Migrant" in a broad sense.** Includes legal migrants (work, student, entrepreneur and family visas) and even tourists. Example: a Schengen visa for a one-week trip to Paris requires extensive personal, financial and biometric data plus a fee, often handled by a private contractor with unclear cybersecurity and accountability.

Chapter roadmap. Chapter 1 sets out the theory. Chapter 2 covers data, Chapter 3 smart borders, and Chapter 4 digital identity. The book's added contribution is linking smart borders (collecting and analysing data) with digital identity (where, how and by whom data is kept).

Chapter 1: Migration and (Surveillance) Capitalism (pp. 16–45)

Argument. Surveillance capitalism is no longer just a Silicon Valley business model. It is a structural feature of today's capitalism. Migration shows this most clearly: an oligarchic alliance of firms and security bureaucracies uses surveillance technology to select, steer and discipline the global working class.

Why bring capitalism into it?

- **The same policies everywhere.** The same approaches and technologies appear in the US, Canada, the EU, the UK, Israel and Australia. Periphery and semi-periphery states (Turkey, Mexico, Saudi Arabia, Bangladesh, Colombia) follow, showing their dependency on core states. Core "donor" states steer UN agencies and NGOs, and the vendors are global tech monopolies.
- **Many capitalist actors benefit.** It is not only Airbus and Thales (border contracts). Zara, H&M, Renault and Ford gain from cheap migrant labour, and universities and financial firms benefit too.
- **Don't blame individual leaders.** Blaming Trump, Johnson, Erdğan, Frontex or the Greek government implies that replacing them would solve the problem. Democrats and Republicans both support virtual walls, Biden continued Trump's border policy, and EU opposition parties offer no alternative.

Shaping the international working class

- **Capitalism needs migration**, to raise productivity, lower wages and deepen exploitation. It also needs to filter migration: letting in the useful and keeping out the rest. Surveillance technology makes it possible to identify, assess, admit or reject, and then monitor people at scale.
- **Legal categories are becoming meaningless.** Refugee vs migrant, the 1951 Convention, "mixed migration": capitalist labour needs override these distinctions in practice.
- **Corporations as stakeholders.** Border control used to be a public matter, with companies limited to lobbying. Now tech, defence, finance and mobile firms run migrant projects, fund UN agencies as donors (Mercy Corps, GSMA, Mastercard) and help set the agenda.
- **Scale.** WFP serves close to 100 million people, and UNHCR and IOM deal with 80 million+. These programmes reach hundreds of millions.
- **"Banking the unbanked"** is the clearest case of corporate agenda-setting, imposed on UN and aid bodies (Mastercard, 2019). Describing forced migrants as "the unbanked" says a lot. Digital ID serves "know your customer" rules for bank accounts and SIM cards (Slavin, 2021).
- **The humanitarian–development nexus.** Vocational training, entrepreneurship programmes and accelerators all aim to get people working as soon as possible in the place global capital needs them.

Examples of labour selection

- **Camps vs cities depend on each country's place in the division of labour.** In Turkey (advanced supply chains, small workshops), camps closed and refugees work informally without permits. In Jordan, refugees stay in camps and are bused to textile factories in desert "special industrial centres".
- **US resettlement NGOs.** Their funding depends on refugees finding a job within 90 days and leaving welfare, which pushes them into slaughterhouses instead of English classes. An AI algorithm used by NGOs matches refugees to jobs.
- **Germany, 2015.** About 1 million Syrians admitted just before metals-sector collective bargaining. Industrialists reasoned that anyone who could pay smugglers about €10,000 had to be skilled.
- **Ukrainian refugees.** Celebrated but rushed straight into schools and jobs without time to recover from trauma.
- **Nepal.** Visa-free travel to India and the Gulf for low-paid work, but months of paperwork and high fees to study abroad (Thapa, 2022).
- **UK.** Hostile environment for asylum seekers, while skilled and capital-linked routes (Ankara Agreement visa, global talent, start-up, graduate visa) are generous. This reflects finance and rentier capital. Agriculture and hospitality complaints about labour shortages are ignored.
- **EU–Turkey Readmission Agreement.** Turkey keeps Syrian, Afghan, Iranian and Iraqi refugees in return for EU funding. This is profitable for European and Turkish capital and lowers wages in both.

- **Turkey's open-door border with Iran since 2020.** Hundreds of thousands of Afghans, Pakistanis and Iranians cross each year to work unregistered in textiles, leather, construction and agriculture. Many work in supply chains for Zara, H&M, M&S, Primark and Next. The threat of deportation silences them. Unions cannot organise local and migrant workers together. Turkey hosts about 4 million Syrians.
- **Summary example.** "A Syrian person should go to Turkey to work for a global company but must be prevented from going to Germany." Surveillance technology does the filtering.

Collecting data on citizens of other countries

- Work, study and even 3-day tourist visas demand hundreds of pages on finances, bank movements, education and marital status, plus biometrics and a fee. The data goes to private intermediary companies, with no transparency or accountability, and refusals can come without explanation.
- The UK, US and Germany build up data on millions of people from Turkey, China and India. This is effectively an intelligence activity.
- Uses: monitoring permit holders, detecting overstayers, predicting "intent to work informally" on tourist visas, and language and "sham marriage" tests on family visas.
- The author accepts state sovereignty. His objections: selection follows class interests, the analysis happens before people leave home, and far more data is demanded than needed.

Surveillance capitalism: the theory and how the book extends it

- **Zuboff's model (2019).** Platforms (Google, Meta) collect data, predict behaviour and sell targeted ads. Prediction then becomes manipulation to remove uncertainty. States picked this up (floating voters in the Trump and Brexit campaigns). Security and intelligence bodies became clients.
- **From business model to structural feature.** Combined with surveillance, which was always central to capitalism (workplace discipline, schools, the army), the model now covers the whole system.
- **The oligarchic alliance:**
    - Military firms: Elbit, Thales, Airbus
    - Tech: Palantir, Microsoft, robotics and data-mining firms, social media platforms
    - Telecoms: mobile operators, the GSMA
    - Finance: banks, Visa, Mastercard
    - Security bureaucracies: Frontex, UK Home Office, US CBP
    - Academia: EU Horizon and UKRI projects
- **Why call it an oligarchy.** These actors are few, monopolistic and global, with close links to security agencies. Amazon is the largest US defence contractor through Pentagon cloud contracts, and IBM, Microsoft and Palantir compete for defence work. Retired Pentagon generals sit on tech boards and staff move between them. They meet through lobbying, advisory boards, trade

associations and fairs. The work is secret because "security" is sensitive, so there is no transparency or accountability.

- **Coordinated by donor states' security bureaucracies.** Example: technology Elbit tested on Palestinians is marketed to Frontex and the UK on the strength of that "experience". Treating migration as a security issue, alongside terrorism and drugs, keeps it within security agencies.
- **Intelligence continuity.** After 9/11, mass surveillance was legalised. Surveillance capitalism adds forecasting and manipulation, and is partly outsourced to private firms (Véliz, 2020: "Data is a toxic asset").
- **Donors make UN agencies accomplices.** They run "awareness" campaigns to stop migrants heading for Europe. Those who still go meet Frontex and national armies.

Critique of Zuboff

- **Rejects "behavioural surplus".** Users do not create value through unpaid work. The better concept is **rentier capitalism** (Christophers, 2022). Platforms collect monopoly rent: a share of advertisers' surplus value from other sectors. Blitzscaling builds users first and takes profit later.
- Focusing on the user–platform relationship misses how tech firms became infrastructure (cloud, operating systems) for every sector, including the military, finance and the state. **Alternative: public ownership of infrastructure platforms**, not just stronger privacy.
- **Control of leisure time.** Workers won the 8-hour day, which gave them time for politics. Social media now captures non-working time for analysis, advertising and political messaging.
- **For migrants, behavioural surplus is not the issue.** States use surveillance capitalism's power to surveil, analyse and predict. Example: EU border agents seize asylum seekers' phones, and happy celebration photos are used as evidence that they "do not seem to flee persecution". Call detail records, sensors, drones and satellites track movement (Maxmen, 2019; Bircan, 2022). The tech firms earn from serving institutions.

Privacy

- Bauman (1998): "Great crimes often start from great ideas." Border control now happens far from view (the Mexican desert, the Mediterranean, the Iranian mountains, the Greek islands, Nauru), "in a hygienic and remote manner" with no "blood or tears" on our screens.
- **All three technologies (big data, smart borders, digital ID) depend on denying migrants privacy.** Consent is not even considered. That is why migrants are ideal test subjects: surveillance capitalism needs as much data as possible, and privacy gets in the way.
- **Privacy is necessary but not sufficient.** GDPR is still violated, and firms build "privacy-preserving" cryptographic tools that keep the data flowing.
- **Is privacy a "first-world problem"?** No. Véliz (2020): privacy is power. But her argument is aimed at citizens of rich countries, not people fleeing death threats. Weak regulation in the Global South, and its non-application to foreigners in the North, makes these the ideal testing grounds.
- **Deregulation** (Zuboff; Bauman's "universal deregulation") and the promise to tame neoliberal uncertainty fuel demand for prediction.

A new capitalist hegemony

- The literature criticises smart borders but views digital ID positively, or as fixable with technical measures. The book connects them.
- Monopolies, donor states, UN agencies, humanitarian bodies and academia together form a **new capitalist hegemony in migration**, with no democratic oversight. The post-war legal order is denied or ignored ("asylum should have been claimed elsewhere").
- Statistics such as "1 billion people without ID", "80 million forcibly displaced", "100 million facing hunger" and "1 billion climate migrants in a decade" are opportunities from capital's point of view.
- Effects: bringing people on the margins into capitalism as workers and consumers, and weakening wage demands of existing workers. Bonus: anger is directed at newcomers rather than at capitalism.
- **Practical takeaways.** Consider rejecting projects that involve surveillance-capitalist firms at the outset. Be careful with projects that feed the hegemony even if they solve real migrant problems. Build counter-hegemonic, migrant- and worker-centred innovation. A coordinated front needs an equally broad response, linking migration with climate, poverty, inequality and conflict.

Chapter 2: Migration and (Big) Data Analysis (pp. 46–67)

Argument. Data analysis underpins every surveillance technology in the book. Big data on migrants is mostly collected by capitalist firms, coordinated by the security state, and increasingly supplied by humanitarian agencies. In the process, privacy, consent and the "no harm" principle are dropped, and migrants are reduced to workers to be monitored.

Corporate dominance over data

- Mobile operators, financial firms, platforms, social media, search, translation and navigation apps collect real-time migrant data continuously. Vodafone, Orange, Mastercard, HSBC, Meta and Google can track migration across countries (Weber, 2022). Personal example: as a Turkish-speaking migrant in the UK, the author is shown remittance ads.
- **Fieldwork evidence.** Mobile operator officials in Turkey, speaking anonymously, said they share refugee data with security and intelligence units daily. There are similar claims about Bangladesh and one warring side in Yemen.
- **Firms can monitor and steer people on the move better than states or UN agencies.** Researchers hope firms will share data, but rarely question their dominance (Bircan and Korkmaz, 2021).
- **Data brokers** are the most secretive players and need scrutiny in high-migration regions.
- **"No harm" means nothing to profit-seeking firms.** Their priority is turning people into labourers, customers and data sources.
- **The security state coordinates in the background.** It gets data from social media and operators, and from smart-border tools (satellites, sensors, robot dogs, drones, fake phone towers). "Know

your customer" and anti-money-laundering rules pull banks and operators into surveillance (Slavin, 2021).

The data and the setting

- **Two sources.** Historical data (past visa and permit applications) is used for categorisation and risk scores. Real-time data comes from satellites, drones, sensors, the internet of things, social media and phones.
- **Scale.** Tens of millions in contact with UNHCR, WFP and IOM, millions of legal migrants, and hundreds of millions of hosts (e.g. Bangladesh and the Rohingya).
- **Most migration is South–South**, into poor countries with weak data protection and little power over tech giants. Phone operators gather more daily data than states can manage in a census. This reproduces dependency and colonial ties.
- **Spillover to local populations.** Aid-linked fintech and telecom products roll out to host communities too.
- **Migrants are valuable customers.** GSMA (2018): migrants use phones and social media more than locals. The paying clients are UN and aid agencies spending donor funds, but the data itself is the prize: "untouched communities" are training data for algorithms.

The humanitarian sector as data supplier to tech companies

- Donors push digitisation (data science, AI, mobile money, blockchain) for "transparency and efficiency" but do not fund in-house capacity. They often require working with their own countries' tech firms. Agencies end up depending on corporations.
- **The roles have flipped.** Firms used to be suppliers to aid agencies. Now aid agencies supply data to tech, finance and telecom firms (Hosein and Nyst, 2013; Taylor and Meissner, 2020).
- **Frontline workers in crises** register and verify recipients, run questionnaires, gather consent, and hand out SIM cards and prepaid cards. This brings people into corporate view, often under chaotic, life-and-death conditions. Examples: Yemen, Syria, Afghanistan, Rohingya in Bangladesh, Syrians in Jordan, Lebanon and Turkey, Nigeria, Kenya, Nepal.
- **Firms gain without sending staff** to Yemen, Afghanistan, Haiti or Nepal, using public money. This erodes humanitarian autonomy.
- **WFP–Palantir (2019).** WFP feeds close to 100 million people. It signed with Palantir, a firm that works with the CIA and Pentagon, whose boss advised Trump, and whose technology is linked to migrant deaths. That gave it access to data from a supposedly impartial UN agency. Nuance: a UN agency cannot blacklist bidders, and Microsoft or IBM, which also serve the Pentagon, would have drawn less criticism. Speculative aside: Huawei would never have won, even with a better offer. The real alternative is in-house UN capacity, which donors will not fund.
- **WFP vs the Houthis (2019).** The Houthi government claimed WFP data reached Saudi Arabia and helped target airstrikes. WFP paused aid, then resumed after negotiations.

- **Other breaches.** UNHCR Rohingya data shared with Bangladesh. US-collected Afghan data fell into Taliban hands. **IFRC hack (January 2022)**: data on 550,000 people stolen, likely by a state actor.
- **Interview with a tech provider (2021).** It serves 30+ aid organisations and holds data on about 100 million beneficiaries from 40+ countries. It says it follows GDPR, but there is no way to verify this and no regulatory checks.
- **Effects on the sector.** Short-term projects, high staff turnover, CEOs focused on donors, NGOs run like project-management firms. Migrants become "beneficiaries", not participants. Accountability runs to donors, not to migrants (Duffield, 2012). Long-term camp residents in Jordan, Bangladesh, Uganda and Kenya work without legal worker status.

Academic debates: three concerns

1. **Good intentions, wrong audience.** Big-data migration studies aim at integration and readiness, but their audience is authorities who already want to stop migration. Early warning of a movement leads to walls and troops, not food and shelter, and can raise death rates. The author's earlier work: *Data Science for Migration and Mobility* (2022, with Albert Ali Salah and Tuba Bircan).
2. **Data scientists without migration expertise.** They miss theory (e.g. the new economics of labour migration: migration as a family decision, remittances as insurance). Job-matching algorithms recommend roles that need no language skills. Settling migrants in "sympathetic" towns ignores that attitudes change (e.g. Poland's shift towards Ukrainians) (Bansak et al, 2018).
3. **Digital inequality and ethics.**
    - New arrivals on the Greek islands ask for SIM cards before food (Latonero et al, 2018), but many migrants, especially low-skilled people and women, lack smartphones, 3G or credit.
    - Some deliberately avoid phones, camps or registration to stay invisible.
    - Crowdsourced disaster data (Haiti, Nepal) is skewed towards better-off people: "like dealing with a disaster in New York with data only from Manhattan."
    - Researchers using corporate datasets have no relationship with the people in them. "Consent" is a clause in SIM-card terms and conditions. Full anonymity is impossible (Véliz, 2020).
    - **Group harm:** even anonymised analysis of a movement can be used against everyone in it. Example: in a Turkish phone-operator data challenge, researchers spotted migrants working informally on a large infrastructure project and left it out of the report to protect their jobs.

Consent, privacy, manipulation

- **Consent becomes meaningless.** Technology choices are made by donors and firms before funding, infrastructure and hiring. Migrants are asked to consent only at the end. "Meaningful consent" requires real alternatives, which do not exist.

    - **Zaatari camp, Jordan:** blockchain-based aid, and iris scans to pay at camp shops (Juskalian, 2018). Refugees' main worry was whether the scan would damage their eyes.
    - **Nigeria:** prepaid-card passcodes could not be used by people who could not read. Shape-codes were then entered upside down, so a human figure was added to show which way was up. Technology made a simple process harder.
    - Some people refuse registration and lose aid. Some burn their fingertips to avoid fingerprint records.
- **Privacy.** Raising privacy objections means losing an application or aid. Privacy is power, not a private matter (Véliz, 2020).
    - **European Space Agency:** satellites can identify the book a person is reading. ESA tracks migration from origin to destination and **sells the data** to firms, researchers and political groups. Migrants can spot drones and robot dogs, but not satellites (Bircan, 2022).
- **Manipulation.** Australian and US YouTube ads in Afghanistan and Latin America: "Don't even think about coming to our country." Ads for remittances, citizenship and language classes. Phones are seized at EU, UK and US borders, and posts and photos treated as evidence of "real" asylum seekers vs "economic migrants" (Riotta, 2020; Rohrlich, 2020). This is a gap in the literature and a planned future study.

Predicting migration

- **UNHCR goats.** Somalis sell goats before leaving and buy new ones in Ethiopia. Falling Somali and rising Ethiopian goat prices signal mass movement.
- **EU Agency for Asylum (Malta).** Forecasts irregular movements from Africa, the Middle East and, since 2022, Ukraine, reportedly about one month ahead, working with tech firms and security bodies.
- **Big data underlies everything.** Surveillance capitalism (predict and manipulate), security intelligence, smart borders (collect, analyse, act) and digital ID (collect and store) all depend on it.

Chapter 3: Smart Borders (pp. 68–86)

Argument. Smart borders let states detect and stop migrants before they reach the physical border. They are built mainly by military firms working with tech firms and security bureaucracies, and tested on migrants with public money. The same products ease mobility in some places and kill in others. They militarise borders, threaten peace, and reproduce racial and colonial hierarchies. Even "pro-migrant" resilience projects funded by the same states extend capital's reach.

What "smart borders" means. AI, drones, facial recognition, biometrics, satellites, sensors, and phone and social media analysis that work beyond the physical line. Elbit's Arizona system detects people 7.5 miles from the border. Anduril's laser-enhanced AI cameras detect all movement within 2 miles and tell humans from animals (Feldstein, 2019).

Two core concerns. (1) If the technology works on migrants, it will be used on whole societies (lie detectors are the test case). (2) Because military and arms firms build it, borders are militarised, cross-border intelligence grows, and peace is put at risk.

Same technology, opposite outcomes

- **Norway–Sweden:** a 1,000-mile frictionless border. Automatic number-plate recognition (ANPR) and scanning let about 70% of freight trucks cross without stopping.
- **Turkey–Greece, US–Mexico, Italy and Malta–Libya:** the same kind of products are lethal. Malta's use contributes to Mediterranean deaths and Libyan slave camps.
- **Legal migrants:** AI streamlines visas for applicants from "non-risky" countries (e.g. Canada) and supports asylum caseworkers (e.g. Germany: assessing applications, transliterating Arabic names; a human still decides) (Bankston, 2021).
- **The explanation is not that Norway is kind.** It is capital's interest: goods and capital move freely, while labour mobility is managed. The same companies, with the same aims, operate in both settings.

Why the border is a testing ground

- **The military origins of tech are back.** The claim that Silicon Valley "democratised" technology development misses how tech firms rejoined the military-security complex. Border management is fertile ground (Larsson, 2020). Weapons testing is rare and secret, but border products are deployed constantly and in quick succession.
- **Real-time data is what drives surveillance capitalism** (Google search and maps, Amazon shopping, Meta posts). Controlling mass movement shows it has become a defining feature of capitalism, not just a business model.
- **The same tools serve predictive policing** and suppressing protests (Milivojevic, 2021). Authoritarian states such as **Uganda** buy "border" tech to monitor opposition. Exports to dependent states keep their regimes in power and deepen neo-colonial dependency and data control.

Testing and money

- **Israel/Gaza.** Israeli firms market products as "successfully tested" on Palestinians. Gaza is an open-air prison used as a test site.
- **Greek island camps (2021).** The EU paid **€43 million** for the Samos camp. Biometrics, cameras and sensors everywhere. Every movement is analysed by AI and threats are reported to a control centre in Athens (Molnar, 2021a, 2021b).
- **US.** The border and immigration budget is up **6,000% since 1980**. **$223 million** in 2019 for Homeland Security border technology. **Northrop Grumman: $95 million** (2018) for a DHS biometric database, stored on AWS. **RAVEn (DHS, $300 million):** AI for social media mining, biometrics and location data to flag non-citizens (Mijente, 2022). **US Marine Corps–Anduril: $13.5 million** (2019) for automated detection along 30 miles of the border. This started under

Obama, expanded under Trump with Silicon Valley, and continued under Biden. Firms involved: Palantir, Amazon, Salesforce, Microsoft, Dell, HP (Mijente, 2019).

- **EU. €34.9 billion** for 2021–27, up from **€13 billion** for 2014–20. **Frontex–Airbus: €50 million** for aerial surveillance, plus military-grade drones and pushbacks. People are forced onto deadlier routes.
- **UK.** ADS (the arms lobby) set up an Industry Reference Group with the Home Office. **Future Borders and Immigration Systems (2020): £113 million.** BAE Systems (2018) and CACI (2020) tenders of £4.9 million each. **Tekever** (Portuguese) drones over the Channel (January 2021). **Cellebrite** (Israeli) extracts all data, including deleted data, from migrants' phones (Privacy International, 2021).
- **Facial recognition.** Banned in some US states but spreading. Higher error rates for minority ethnic groups. The market is expected to reach **$12 billion by 2028**, with migrants as test subjects (Kelly, 2022).
- **Those who make the bombs make the border tools.** Lockheed Martin, Airbus, Safran and Thales, plus IBM, Amazon, Microsoft, Fujitsu and Accenture (Achiume, 2020).

Side note on Palantir

- **WFP data on 92 million+ beneficiaries in a $45 million deal** (Achiume, 2020).
- Founded in 2003. Early funding from **In-Q-Tel (the CIA's venture capital arm)**. Founder Peter Thiel advised Trump. Staff move between Palantir and the Pentagon. **Up to $15 million on lobbying (2006–19). $800 million** US military real-time intelligence database (2019).
- **ICE contracts of $150 million+**, including the case-management tool used in **separating parents from children** ($53 million initial phase). **$1.5 billion+** in total across agencies, including the FBI and Navy.
- **Other firms are not much different.** Palantir runs on AWS. Amazon won the **$10 billion** Pentagon cloud contract, making it the largest US military contractor. Microsoft: **$480 million** military VR. **Project Maven** (AI drone targeting) moved from Google to Anduril after staff protests, and Google later dropped its "don't be evil" motto. Anduril also builds surveillance towers for the UK Royal Marines, US Marines and CBP.

Speculative academic projects

- **AVATAR** (Automated Virtual Agent for Truth Assessments in Real Time): kiosk AI lie detector reading eye, mouth and hand movements, tested in Canada, the US and the EU (Daniels, 2018).
- **QinetiQ** lie detector (UK defence firm), funded by the EPSRC.
- **iBorderCtrl:** Manchester Metropolitan University, **€4.5 million** Horizon 2020 grant, affect recognition tested in Greece, Hungary and Latvia.
- **UK Border Agency Human Provenance Pilot:** DNA and isotope analysis to determine asylum seekers' nationality.
- These are publicly funded "research", carried out largely in secret.

Tech firm or military firm?

- Amazon, Microsoft and IBM compete to serve the Pentagon and CIA, build autonomous weapons, and have ex-Pentagon and CIA staff on their boards. **They cannot be separated from military and finance capital.**
- Lenin's definition of imperialism (industry and finance capital merged in an oligarchy) now includes global tech firms. Migration accelerates that merger, and prejudice against migrants allows more reckless testing.

Threats to peace

- Drones decided the Armenia–Azerbaijan and Russia–Ukraine wars. Robot sentries are coming. Cyber-weapons and AI were used in the attack on Iran's nuclear facilities, the assassination of an Iranian general, and Pegasus.
- States surveil beyond their borders (in the name of migration), collect foreigners' data through visas, and can intervene in other countries through platforms. Peaceful conflict resolution is weakened.
- Capitalism tends towards war over markets (Lenin). Surveillance tech converts quickly to weapons.
- **Paradox:** virtual borders can be hacked or fail, making borders more vulnerable (Kello, 2019). States that buy technology they did not build depend on foreign licence-holders, who can shape conflicts.

Reform or abolition?

- **Racial capitalism.** Colonial hierarchies are built into deep-learning systems. Violence is carried out remotely and "hygienically" (Gilroy, Mbembe, Benjamin). Black-box AI cannot be fully audited, so reform through transparency is unrealistic.
- **Schulz (2022):** rights-based reform is "techno-liberal" and does not question the system. Automating an unjust system makes it worse. She calls for redesigning the whole process around migrants.
- **Frontex.** Under criticism since 2020. Director **Fabrice Leggeri resigned in 2022** after evidence that it left people to die, gave Greek authorities coordinates for pushbacks, and guided the Libyan coast guard. He called Frontex "not a welcoming committee" and seemed to see it as the core of a future EU army.
- **Colonial examples.** Drones and satellites spot boats heading for Malta and Italy and alert the Libyan "coast guard", controlled by a warlord, even in international or Maltese waters. Migrants end up in **Libyan slave camps** while the EU keeps funding. Greek camps act as labs for facial recognition and emotion AI on African, Middle Eastern and South Asian asylum seekers.
- **The key question:** should the goal be facial recognition that is equally accurate for all ethnic groups, or opposing its use by military, intelligence and security bodies altogether?

Denial of privacy

- Phones seized, deleted data recovered. Happy wedding photos are used to argue "not fleeing". Deleting them is read as "admitting it". Protecting fellow travellers or hiding contact with smugglers is treated as aiding and abetting, even though refugees usually *must* cross irregularly.
- **Border externalisation.** The EU predicts from satellite, social media and phone data whether people leaving central Africa are heading for Europe or moving within Africa (most African migration stays within Africa). It shares this with transit states. Neighbourhood agreements transfer border technology, making Morocco and Tunisia buffer zones (Andersson, 2022). Turkey plays the same role through the readmission deal.
- Boat crossings are a small share of migration. Many irregular migrants are visa overstayers, so **legal migrants are surveilled too**. Biometrics lay the groundwork for permanent monitoring. Migrants give up privacy to get residence, then citizenship.

Denial of the right to asylum

- You must cross a border to claim asylum, and irregular entry is not a crime for refugees. There is **no legal "first safe country" requirement**, yet the UK plans returns to safe third countries or **Rwanda**. Frontline states (Turkey, Greece, Italy) object to the unfair burden. Resettlement promises (Dublin, US pledges) go unmet.
- Smart borders deny asylum in two ways: detection (drones, satellites, sensors) and building cases against applicants (phone searches, lie detectors).

"Resilience": externalisation dressed as development

- Resilience is imposed on the Global South to keep people where they are, never preached to rich societies, which reflects a colonial and racial logic (Bigo and Guild, 2005).
- **Innovation requirements bring in firms.** Mobile cash transfers send donor money to banks, telecoms and tech firms, along with new customers and data.
- **The biggest "AI factory" is in a camp in central Africa.** Displaced people label images for Big Tech machine learning, which is cheap and good PR. Similar work happens in Jordan and Lebanon.
- **Jordan.** Desert textile special economic zones failed because refugees preferred informal city jobs. From 2018, aid bodies backed start-ups and the gig economy (e.g. Uber). Men drive taxis. Women sew, clean and cook at home, following gender roles.
- Success is measured by jobs and income, but this is no proof of resilience, and education, health and environmental problems remain. **Lesson: look critically at apparently pro-migrant projects too.** They are funded and built by the same states and firms. This leads into Chapter 4.

Chapter 4: Digital Identity and Surveillance Capitalism (pp. 87–115)

Argument. Digital identity is the hardest case because it is presented as pro-migrant: access to aid, rights and financial inclusion. In practice it complements smart borders. Smart borders decide who crosses and how far they go. Digital ID stores the data and monitors the people who are let in, turning them into

workers, customers and data sources. Tech and finance firms test blockchain and biometrics on refugees with donor money. Promised decentralisation often produces the most centralised systems of all.

Why it is harder to criticise. On smart borders, the lines are clear (security vs rights). On digital ID, a reformist consensus dominates: everyone agrees a technical fix can make IDs more secure, crypto-based, decentralised, "user-controlled" or "self-sovereign" (FATF/OECD, 2020). The field is also more transparent and more interdisciplinary than the secretive smart-border sector.

The real need for identity

- **1 billion+ people have no official ID** (UN). ID is part of the SDGs. Without it, rights are hard to claim, and so are bank accounts, SIM cards and internet access under "know your customer" rules (Slavin, 2021). For corporate agenda-setters, the undocumented are a big market.
- **Why people lack ID.** (1) Deliberate political exclusion (Kurds in Syria, Rohingya in Myanmar). (2) Lack of state capacity (difficult terrain, nomadic lifestyles, late registration of newborns, especially girls).
- **Refugees' problems.** Documents are lost, forged, not recognised, or held by only one family member. **Mosul after ISIS:** competing Ottoman-era, Saddam-era and ISIS-era deeds to the same house, all genuine.
- **States differ.** Turkey quickly issued ID numbers giving access to education, health care and work permits. Many states cannot document their own citizens.
- **The case for digitising.** It prevents fraud, duplicate claims and confiscation of IDs from women, children and disabled people. It lets agencies share data and avoid duplication. Venezuelans and Latin Americans moving through several countries can receive aid in different places.
    - **Somalia:** each NGO hands out its own SIM card, so recipients carry several, and operators are paid many times over.
    - The **Taliban seized US-built digital ID records.**
    - **Ukraine's e-government system** let refugees download IDs, diplomas, transcripts and health records for host states.

Digital ID in integration: completing the smart border

- Recap of labour positioning: Afghans and Syrians to Turkish textile and food supply chains, Nepalis to Gulf construction and tourism, Filipino women to domestic work in Canada and Germany, Turkish and Indian IT and health workers to the UK and US, Pacific islanders to Australian rugby.
- **Smart borders alone cannot turn migrants into workers.** Digital ID controls life after the border: bank accounts, SIM cards, internet access, online obligations, consumption, continuous data generation, health care (to keep workers productive) and school enrolment (to free up adults to work and train the next generation of workers).
- **Together they let surveillance capitalism monitor the whole process**: the journey, settlement, integration, value creation, and continuing ties with home (remittances, visits, new arrivals, trade).

Digital ID in humanitarian emergencies

- **Humanitarian–development nexus.** Aid cannot last forever, so the aim is self-reliance.
- **Cash vs in-kind aid.** Identical aid packages are wasteful (no need for sanitary pads in families without women, or nappies without babies). Cash lets people choose and supports local markets. But physical cash is risky (theft, bribes, price-gouging, patriarchal control over spending), so **mobile money** is used. That requires phones, SIM cards, credit, internet and bank accounts, which brings in operators, banks and tech firms. Donors like it because it is traceable and auditable.
- **In-kind aid needs no ID. Digital cash does.** "Know your customer" rules force identity verification and new digital IDs, shared with operators and banks.
- **Commercialisation of aid.** Firms get two kinds of customers: UN agencies and NGOs (buying the infrastructure), and millions of recipients (using phones and accounts). They then expand to local populations. Firms register thousands of people without a single employee on the ground, because aid workers hand out cards and collect biometrics. This is low-risk, publicly funded market entry.

"Recording an entire life"

- A refugee's digital ID records far more than name and birth details: all aid received, all spending, call records (revealing socio-economic and cultural traits), workplaces, children's schools and family certificates. Over the years, **identification becomes infrastructure for recording every moment of a person's life.**
- **WFP: 100 million people. Palantir provides the infrastructure, plus financial firms and operators.** "A gold mine for surveillance capitalism": public money, new markets, data that no other monopoly has, and little privacy law. **Issuing the ID is the first step. Years of data extraction follow.**

Digital identity in general

- Everyone has many digital IDs (bank, university, employer, Gmail, Facebook, news sites), arranged in a **hierarchy** (e-government and banking at the top, Gmail used to log in elsewhere).
- **Foundational IDs** (issued by the state, proving who you are) vs **functional IDs** (for specific services: driving licence, banking, social media) (Slavin, 2021). Refugees need foundational IDs, but **surveillance capitalism's need for data is met by functional IDs.**
- **Why humanitarian settings lead on ID innovation.** The "no harm" principle and growing demand for privacy force agencies to demand safeguards. So the most advanced and speculative work (self-sovereign and decentralised IDs, blockchain, biometrics) happens here, with pilots in the Global South by start-ups and monopolies such as Microsoft (Cheesman and Slavin, 2021).
- **The pattern.** Lie detectors spread to schools and workplaces, border drones prepare for future wars, and blockchain and biometrics are piloted on refugees. Pilots fail and are replaced by new models, but the exploitative neo-colonial attitude stays. Refugees have no input at any stage.

- **The paradox of privacy-preserving technology.** A more secure, cryptographic product sold by a dominant firm protects against small-scale attacks but *deepens* surveillance capitalism and monopoly. **Oxford observation:** academic tools against disinformation, for privacy or against bias end up commercialised through Microsoft, Meta or Amazon, "expecting the solution from the very actors that have created the problem."

Leading organisations (the ID oligarchy)

- **UK:** about 10% of the population ("a market of 7 million") cannot prove their identity online (Soprano, 2022). Verification is only the start of continued data collection.
- **World Bank:** the main champion, "with a missionary zeal". **World Economic Forum** works alongside it. **EU** support is shaped by national concerns.
- **ID2020:** a lobby founded by monopolies including **Mastercard and Microsoft**, focused on the Global South and humanitarian settings.
- **GSMA** (mobile operators, e.g. **Vodafone, Orange**): runs digital ID projects, some specifically for refugees.
- **The UN SDGs** give the legitimacy that lets these firms lead.
- **EU–US biometric "race" (really cooperation).** eu-LISA and Frontex visited US CBP in Washington (June 2022). US in-car facial scanning success rose from 40% to 76% with a second camera (Monroy, 2022). The **EU Entry/Exit System** aims at 400 million people (four fingerprints plus face), on top of SIS, Eurodac and VIS. The US holds biometric data on about 275 million.
- **HART (DHS, $6.16 billion).** Face, DNA, iris, fingerprints and voice. Built by **Northrop Grumman and Veritas Capital**. Buys data from **Clearview AI** (fined for scraping social media photos without consent). Hosted on **AWS GovCloud**. Usable against protesters: counter-insurgency facial recognition from Iraq and Afghanistan was used on **Black Lives Matter protesters in Baltimore** (Mijente, 2019).
- **Externalisation:** the EU Emergency Trust Fund for Africa paid **€53 million (2016)** for a fingerprint database in **Mali and Senegal**, built by **Civipol** (40% French state, plus Airbus, Safran and Thales).

Biometrics and blockchain: promises vs practice

- **The promises.** Biometrics replace documents and are hard to fool. Blockchain offers cryptographic security, decentralised and federated governance, no bank fees, and accountability to donors. **Zaatari, Jordan (WFP closed system):** women scan their irises at shops and pay from their own blockchain wallets. Public Ethereum was used after the Nepal earthquake.
- **Hype.** Before the pandemic, blockchain was added just to win funding. **Interview:** one aid agency could not open its own blockchain-encrypted data and asked the tech firm to **decrypt it into a spreadsheet**, which defeats the point.
- **Donor innovation requirements** (US, UK, Norway, Sweden, Germany, Japan). Buzzwords such as security, privacy, empowerment and integration lead to proposals written at headquarters rather

than from the ground up. Agencies cannot build technology themselves, so they partner with firms, and the bigger the partner, the better the funding odds. The firms dominate design and implementation, and the NGO ends up secondary. Projects run in Nigeria, Kenya, Nepal, Turkey and Thailand, sometimes with no basic internet.

- **How it works vs reality.** Blockchain needs each user to hold a private key. Refugees cannot realistically keep long keys safe, mistakes cannot be undone, and lost keys mean permanent loss (like bitcoin owners locked out of fortunes). **Fieldwork in two African countries and interviews: private keys are not shared with beneficiaries. The tech company holds all of them and carries out every transaction.** Local banks, operators and even the Western NGO lack expertise, so their keys are held centrally too.
- **Result: "the most centralised digital aid distribution system ever"**, more centralised than an ordinary database. **Refugees' digital IDs do not belong to them.** They cannot see or check their own data.
- **Public alternatives.** EU work on blockchain ID, and the **Istanbul Metropolitan Municipality (İBB)** blockchain digital ID for all residents (2021). The author's research project looked at refugees using İBB-held data for financial inclusion. Positives: people could check their own data, and there was a clear legal framework.
- **A closed blockchain means no independent check.** Accountability runs to donors, not the public.
- **Gender.** Separate wallets for men and women, with no joint family accounts, are a top-down, orientalist, "white man's burden" approach. It ignores families that budget together and the many cases where women already manage the household budget.
- **Overall:** more centralisation, less transparency, less accountability, the opposite of what was promised.

Consent, privacy and alternatives

- The same problems as big data and smart borders: publicly funded pilots that develop more intrusive surveillance.
- **The reformist response.** Weitzberg et al (2021, *Big Data & Society*) call for less polarised dialogue. The Alan Turing Institute works on "trustworthy digital IDs". **Self-sovereign identity** depends on recognition by states and firms, and on digital literacy and status that many lack. Many refugee-first ID start-ups failed or abandoned their principles (Cheesman and Slavin, 2021).
- **The problem is not technical.** Better technology, once commercialised, deepens surveillance. Smart borders ("security") and digital ID ("pro-migrant") share one common denominator: developing and testing surveillance technology on migrants, driven by corporate agenda-setting.
- **Scale:** hundreds of millions of people, or billions if the poor and undocumented are included. Migrants have little legal recourse, Global South regulation is weak, Northern borders are hardening, and hostility to migrants is high. That makes this a "comfortable playground" for capital.

- **No meaningful consent.** By the time refugees are asked, the project is funded, built and staffed. The only alternative is going without aid. Even agency managers may not understand the technology. Nobody, including the firms, knows the long-term risks of blockchain or how long today's encryption will hold. That is *why* it is being tested.
- **Privacy doesn't apply to aid recipients.** Handing private keys to firms shows the real focus is testing efficiency. Refugee data security is secondary. Critical NGOs and start-ups cannot challenge Mastercard, Microsoft, Vodafone, the World Bank or the WEF.
- **Alternatives:** work with public agencies, not just the latest technology. Avoid projects that serve corporate agenda-setting, especially those of surveillance-capitalist firms. Adopt **data minimisation**: collect as little as possible, only when needed, and respect people's right to access their own data.

Conclusion: How Can We Resist? (pp. 116–132)

Argument. Migration, border control and humanitarian aid are capital's "lowest-hanging fruit": weak legal status, sovereignty claims, secrecy and public hostility let firms test their most speculative projects there. Resistance has to go beyond exposing individual firms, separating "good" from "bad" technology, or relying on rights alone. It has to put capitalism at the centre, defend consent and privacy, keep public control of technology, and connect migration to wider struggles.

The system in summary

- **The cycle.** Donor states fund humanitarian or academic R&D. Speculative surveillance technology is built with public money, tested on migrants by security bodies or UN agencies, and then commercialised and sold to other states.
- **The oligarchy.** A small network across the US, EU, UK and Israel, whose people move between companies and whose decisions apply globally.
- **Why migration is the testing ground.** Weak legal status, sovereignty claims, secrecy in security matters, and little public sympathy. Firms "do as they please" in the Mediterranean, in camps and in war and disaster zones.
- **What it means for other fields.** Blockchain aid pilots point to the future of finance, crypto and central banks. Robot dogs, long-range sensors, satellites, movement prediction, and facial and emotion AI in camps show how future wars will be fought and how authoritarian control will work. Migration scholars need to talk to researchers on work, war, AGI, surveillance and democracy.

Don't just blame a few bad actors

- It is right to criticise firms, academics building lie detectors, and **universities that send proposals through narrower technical ethics review** to avoid social-science ethics rejection. But this is a systematic alliance.
- **Palantir or Microsoft can do smart borders with the military and crypto-ID for NGOs without any contradiction.** These are complementary ways of deciding who moves and how far (Lyon, 2009).

- Humanitarian organisations, UN agencies and donor security bureaucracies all approve and commission these products.
- Firms profit without risk because public money and academic support cover the cost. Being "tested" in Palestine, the Mediterranean or on the US–Mexico border gives a competitive edge (Talbot, 2021; Tazzioli, 2021).

No "good tech vs bad tech" distinction

- **The UK.** Theresa May's "hostile environment" sits alongside global talent and start-up visas (settlement in 3 years, citizenship in 4). **UK academic strikes, November 2022:** universities warned migrant staff on sponsored visas not to strike, and the warnings worked. Those who get in are also surveilled, underpaid and unable to bargain.
- **Brexit, Rwanda removals and 500,000 migrants admitted in 2022 are not a contradiction.** Surveillance capitalism covers both those pushed back and those let in.
- **Rights alone are not enough.** Surveillance capitalism, neoliberalism and market approaches have no interest in post-war international law, especially for tens of millions of migrants. Focusing on Trump, Johnson, Erdoğan, Frontex or von der Leyen misses continuity (Obama to Trump to Biden). Defending asylum and non-refoulement without analysing capitalism cannot explain the EU deals with Turkey and Libya, the US deal with Mexico, or Palantir, Microsoft and the arms firms.
- **Racism and surveillance are not ends in themselves.** Personalities (Trump, Erdoğan, Thiel, Musk) make for interesting stories but weak analysis. The real issues are relations of production, surplus value, monopoly, imperialism and (neo)colonialism. The core goal is **reshaping the global proletariat**.
- **Legal routes follow labour demand.** Philippines to Canada (childcare), Nepal to Qatar (construction), Turkey to the UK (software, medicine), Jamaica to the UK (nursing). A Nepali student faces an ordeal and may be detained. A doctor may be refused a tourist visa.
- **Aid agencies acting like businesses.** Why would a humanitarian organisation fund start-ups, mentor entrepreneurs and arrange meetings with global supply chains?
- **Turkey example.** More than 4 million refugees in the labour force. Technology makes reaching Greece harder and staying in Turkey easier. "A young shepherd from an Afghan village may start producing leather bags for Zara or Prada." Instant deportation if he complains shows the authorities knew about him all along and effectively condoned his movement.

War and competition

- Capitalist competition for markets leads to monopoly and war. Migrant-source regions (Afghanistan, Syria, Yemen, Ukraine, Somalia, much of Africa) are sites of great-power rivalry and arms supply.
- **Turkey–Greece.** Border technology funded by both states and the EU is officially about migration but really continues their regional rivalry and gathers intelligence on each other. It militarises the Aegean. Are migrant deaths there caused by anti-migrant politics, or by rivalry over markets and waters?

- Universal ID, "banking the unbanked" and SIM cards for all are driven by the data appetite of surveillance capitalism and intelligence agencies.

"Post-consent era?" No.

- **The reformist "realist" proposal.** Drop individual consent; build privacy in by design, with UN agencies and NGOs supervising design and coding for refugees. Similar to unions overseeing HR algorithms.
- **The author rejects a post-consent society.** It means less regulation, more corporate dominance, less accountability, more data and more speculative projects. It is a colonial, top-down denial of agency. "Some things may be difficult to achieve in real life, but that does not make them impossible."
- **Consent and privacy must be non-negotiable.** At the very least, ask for consent and publicly commit to privacy. That creates accountability and room for further demands. Handing privacy duties to firms such as Microsoft means "expecting the solution from the creators of the problem" and testing their cryptography on migrants.

When the system fails

- Critical scholars often lack technical knowledge, so the downsides of "successful" systems go undiscussed.
- **Eurodac 2020 Annual Report: 1,300 "wrong hits"** (74% from Hungarian data) and **67 "missed hits"** (35 from late Spanish submissions). About 1,400 asylum applications affected, reported as an ordinary technical issue, with no information on what happened to the people.
- Hacked or failing virtual walls also threaten state security (Vukov and Sheller, 2013).

Alternative technology?

- **How migrants use technology.** Smartphones, WhatsApp, Facebook, Telegram and TikTok, maps and translation apps (Gillespie et al, 2016). "Skype mothers" (Filipino domestic workers). Diaspora campaigns.
- **Counter-uses.** Apps that avoid Big Tech or smugglers. **Sea-Watch** uses open and commercial satellite data to reach boats before coastguards do. Migrants rate smugglers in "TripAdvisor-style" groups, change group names often and plan only with people they know. Information is power: e.g. after crossing from Iran into Turkey, people can go straight to UNHCR in Ankara without a smuggler.
- **Technology has both use-value and exchange-value.** Separate those who create value from those who profit. **Don't romanticise migrants' use of technology.** The system still dominates, and migrants in the UK get targeted remittance and citizenship ads, face wage gaps, and have to update biometric data at every renewal.

Moving forward: the proposals

1. **Treat political problems politically.** Open debate that includes migrants. More advanced technology means more dependence on monopolies and security bureaucracies. Stronger encryption is not the answer to privacy concerns.
2. **Reject surveillance capitalism, not digital technology.**
3. **Use "no harm"** to exclude firms that profit from the surveillance-capitalist model and train algorithms on beneficiary data.
4. **Use "neutrality"** to bar tech firms that work with arms makers and military or security agencies from humanitarian and migration work (ICRC and Privacy International, 2018).
5. **Build in-house technical capacity.** Large, long-term operations (hundreds of thousands to millions of people over years) should have their own technical teams and products. These are easier for beneficiaries and fieldworkers to understand, have consent and privacy alternatives built in, and can use feedback. Some NGOs already run their own software for millions of people.
6. **Widen the coalition.** These technologies will reach everyone and fuel militarism. Researchers on surveillance capitalism, tech monopolies, war and work should study migration technology. "It is impossible to mount an effective opposition without making capitalism part of the discussion."

Panel quick reference

The book answers each of the NYU panel's motivating questions. Below, each question is paired with the book's answer and the strongest example to use.

Panel question	The book's answer	Best example to cite	Where
How is AI used in immigration policy and enforcement?	Three linked layers: big-data prediction and risk scoring, smart borders that stop people before they arrive, and digital ID that stores data and monitors those let in	EUAA forecasts movements about a month ahead; Elbit's Arizona towers see 7.5 miles; Zaatari iris-scan payments	Ch. 2–4
What functions and use cases are being developed?	Lie detectors, affect recognition, facial recognition, phone extraction, DNA nationality tests, social media mining, blockchain wallets	AVATAR, iBorderCtrl (€4.5m Horizon 2020), Human Provenance Pilot, Cellebrite, RAVEn ($300m)	Ch. 3
How does AI push government into new functions (combining data)?	States collect data on foreigners at scale (an intelligence function). Aid agencies become data suppliers to Big Tech. Operators share refugee data with security services	Mobile operators in Turkey sharing refugee data daily (author interviews); WFP–Palantir; HART buying Clearview data	Ch. 1–2, 4

Panel question	The book's answer	Best example to cite	Where
Algorithmic decisions with little appeal?	The "metaphysical" view: machine decisions are accepted as neutral. 80% confidence still leaves 20% wrong. Errors are treated as technical issues	Eurodac 2020: 1,300 wrong hits and 67 missed hits, with no account of what happened to the people	Intro, Concl.
What does this mean for privacy and civil liberties?	Privacy does not apply to migrants. Consent is meaningless without alternatives. The tools spread to citizens	Border tech used on BLM protesters in Baltimore; Uganda; phone photos used against asylum claims	Ch. 1, 3, 4

Lines to quote

- "Migrants may be the canaries in the coal mine of a much wider turn toward intimate exploitations of life itself." (Andersson, 2022, quoted in the Introduction)
- Surveillance capitalism is "not simply a business model" but "an intrinsic component of contemporary capitalism". (Conclusion)
- "A Syrian person should go to Turkey to work for a global company but must be prevented from going to Germany." (Ch. 1)
- The same product "that facilitates faster border crossings in Norway may lead migrant people to drown in the Aegean." (Conclusion)
- Blockchain aid ended up as "the most centralised digital aid distribution system ever". (Ch. 4)
- Privacy-by-design through big firms is "expecting the solution from the creators of the problem". (Ch. 4, Conclusion)
- Migration is "the lowest-hanging fruit" for these corporations. (Conclusion)

Your own fieldwork, as first-hand evidence

- Turkish mobile operator officials: refugee data shared with security and intelligence units daily.
- A tech provider holding data on about 100 million beneficiaries from 40+ countries for 30+ NGOs, with no external checks.
- Blockchain aid projects in two African countries: the tech firm held every private key.
- An aid agency asking for its blockchain data to be decrypted into a spreadsheet.
- A Turkish data challenge in which researchers held back a finding that could have cost migrants their jobs.
- The İBB (Istanbul) public digital ID project: a positive counter-example.

Updates since publication (2024) to mention. ICE's ImmigrationOS (Palantir, about $30m) and the Mobile Fortify facial recognition app. The EU Entry/Exit System has been fully live since April 2026. The EU AI Act's high-risk border rules have been delayed to December 2027. These show the book's predictions coming true.