

THE UK'S PRIVATISED MIGRATION SURVEILLANCE REGIME: A rough guide for civil society

February 2021

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission.This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;
- You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright.

For more information please go to www.creativecommons.org.

Photo by John Rodenn Castillo on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

INTRODUCTION 5

1. WHO'S INVOLVED? 7

a. Home Office 8

b. UK Visas and Immigration 8

c. The Border Force 8

d. Immigration Enforcement 9

e. Her Majesty's Passport Office 9

f. Digital, Data and Technology 9

2. "BACK-END" SYSTEMS 10

a. Existing Databases of Relevance 11

b. Databases of Relevance in Development 14

i. Digital Services at the Border (DSAB) / Future Borders and Immigration Systems (FBIS) 15

ii. Immigration Platform Technologies (IPT) 19

iii. Home Office Biometrics (HOB) 21

iv. National Law Enforcement Data Programme (NLEDP) 22

3. "FRONT-END" TOOLS 24

a. Mobile Scanners 25

b. Status Checking 29

c. Border Surveillance 30

d. Language analysis 31

e. Mobile Phone Extraction 32

f. Hacking 34

g. Wi-Fi Analysis 35

h. Communications Data Surveillance 35

i. Surveillance Vans 36

j. Intelligence Sharing Software 36

k. Data Analytics 37

l. Data Analytics 37

m. Data Brokers 38

4. INTERNATIONAL OPERATIONS 40

a. International Biometric Data Sharing 41

b. Surveillance outsourcing 43

5. RESEARCH RESOURCES 45

6. LIST OF COMPANIES MENTIONED IN THE GUIDE 47

INTRODUCTION

The ability to police and 'control' the UK's borders was a central issue for voters in the UK Brexit vote, and is once again headline news with coverage focusing on migration across the Channel.

Regular stories of the Home Office losing track of "foreigners" or having "no clue how many illegal immigrants there are" feed a notion that the UK's immigration system is fundamentally 'broken'.

Perceived and real failures of how the UK tracks people in the immigration system are vulnerable to simplification and dangerous rhetoric in part because of its opaqueness. Already managed and enforced by a confusing complex of government departments, agencies, infrastructure, and contractors, the situation is not helped by the fact that many of the key actors involved are resistant to transparency and that Brexit is demanding yet more changes.

There is no doubt there are severe problems at the Home Office, something recognized by numerous oversight bodies and inquiries. Windrush and the fact that people who rely on the asylum system are left waiting longer than ever are two examples.

But far from being powerless or weak, the reality is that the system is vast, with annual expenditure exceeding £2 billion. UK authorities are able to call on intrusive surveillance powers matching those of anyone else in the world. Immigration agencies are equipped with advanced tools of surveillance, and supplemented by a 'hostile environment' which extends the duty of controlling borders to landlords, employers, teachers, and doctors.

At the same time however, the Home Office has an abysmal record on delivering IT projects, with the effect that it fails to provide basic and vital services for people while continuing to award lucrative contracts to big arms and surveillance companies which enjoy minimal scrutiny and are seldom held accountable in the public discourse.

Providing a realistic perspective of the powers and technology available to UK agencies and the problems across the system are important for dispelling myths and dangerous narratives.

Below, we try to provide a rough guide to how the UK's borders, immigrations, and citizenship system tracks and spies on people, and which companies profit.

The first section briefly outlines the main departments and units involved. It then describes various databases which are used to process immigration data, track people through the borders, immigrations, and citizenship system, or which are relevant because they enable forms of surveillance by law enforcement or immigration authorities. These are referred to for the purposes of this guide as the "back-end" systems.

The following section then describes surveillance and tracking tools available to officers and agencies themselves, referred to here as the "front-end" tools. A section on international operations which are used to support surveillance in the UK is provided, followed by a list of relevant other resources.

1. WHO'S INVOLVED?

KEY FACTS:

- In 2017-18, the UK Visas and Immigration (UKVI) spent £1.1 billion, but earned £1.6 billion in income from things like charging substantial visa fees

- Immigration Enforcement heads up the investigation of and removal / deportation of people who are in the UK with irregular status. In 2017-18, the department spent £430 million, and had an income of £33 million through schemes involving charging "customers" to comply with immigration rule.

- In addition to the operational departments at the Home Office, a separate entity known as an "enabler" called Digital, Data and Technology which oversees a range of tech projects relating to the immigration and asylum system.

a. Home Office

The Home Office is in charge of the UK borders, immigration, and citizenship system.

In 2019, it issued 3.2 million visas to people around the world: 76% of them were for people who were visiting (2.43 million), 9% for students, 6% for workers, and the rest for family and other reasons. In the same period, 35,566 people claimed asylum in the UK – amounting to the equivalent of just over 1% of the amount of visas issued for other reasons.

A large influence on their operations is the idea that the Home Office is capable of being run as a business: in 2015 it signed up to the idea that it could be 'self-funded' by charging its 'customers'. Predictably, it has since told the Independent Chief Inspector of Borders and Immigration that it has "reigned back on self-funding, moving from an objective for self-funding by 2019-20 to an ambition to increase the extent to which [the borders, immigration, and citizenship system] is funded by those who use its services."

Nevertheless, the policy permeated across the Home Office, pushing agencies to raise fees and charge "customers" for new services.

There are four main operational departments governing this system.

b. UK Visas and Immigration (UKVI) manages visa, citizenship, and asylum applications, and had over 9000 staff in 2019.

In 2017-18, the department spent £1.1 billion, but earned £1.6 billion in income from things like charging substantial visa fees.

c. The Border Force is responsible for managing people and goods entering the UK and collecting revenue from trade crossing the border.

It had just under 8200 staff in 2019. In 2017-18, the department spent £522 million, and had an income of £22 million, from schemes such as charging carriers and people for expedited transit through the UK border.

d. Immigration Enforcement heads up the investigation of and removal / deportation of people who are in the UK with irregular status. The department's stated aim is that it wants "to reduce the size of the illegal population and the harm it causes".

It had over 5000 staff as of 2019. In 2017-18, the department spent £430 million, and had an income of £33 million through schemes involving charging "customers" to comply with immigration rules. For example, employers and local authorities could pay Immigration Enforcement officials to do things like check the immigration status of people, including when they're applying for support from local authorities.

e. Her Majesty's Passport Office (HMPO) issues passports and had over 3600 staff in 2019. In 2017-18, the department spent £263 million, but earned £435 million from passport fees and providing customer service.

f. Digital, Data and Technology: in addition to the operational departments at the Home Office, there is a separate entity known as an "enabler" called Digital, Data and Technology which "designs, builds and develops services for the rest of the department and for government". Made up of around 2500 staff, it oversees a range of tech projects relating to the immigration and asylum system.

2. "BACK-END" SYSTEMS

KEY FACTS

- The Home Office is currently developing several large IT systems which will be used to replace existing systems that track individuals throughout the borders, immigration, and customs system and enable the use of surveillance tools by relevant units and officers.

- Large tech and arms companies compete for supplying staff and vague services to the programme, but provide little insight as to what the firms are actually supposed to deliver.

- By converging facial, DNA, and fingerprint data into a single platform, biometric data will be more easily available to more agencies.

A. EXISTING DATABASES OF RELEVANCE

The following databases are used by various agencies across the UK's borders, immigration, and citizenship system and are referenced later in this guide. Many of these are aimed for security purposes and not for immigration or border management, but may nevertheless be used in some way to that end. This list is non-exhaustive.

- The National DNA Database (NDNAD), which holds around 6.3 million DNA profiles of subjects in criminal cases, some of whom have not been convicted of a crime and profiles of victims, as well as marks from crime scenes.

- The Immigration and Asylum Biometric System (IABS), which holds around 25 million fingerprints and faces, for example collected by UK Visas and Immigration (UKVI), including biographic information, fingerprints, and facial images as part of asylum, visa, or Biometric Residence Permit (BRP) applications. Developed by the tech giant IBM in 2009.

- Law Enforcement and Security Biometrics System (IDENT1), the main criminal fingerprinting database used by law enforcement in the UK, which in 2018 held the biometrics of around 8 million people mostly because they were arrested in the UK, and developed by US arms company **Northrop Grumman**.

- The Case Information Database (CID), the main caseworking and operational database at the Home Office. It is used throughout the Department "to record personal details of all foreign nationals who pass through the immigration system". It is being replaced as it is prone to errors, unstable, and unable to interface with other systems,

- The Asylum Support System (ASYS), containing details about asylum seekers applying for and receiving support.

- Warnings Index: A watchlist developed originally in 1995 which tracks people with "previous immigration history, those of interest to detection staff, police or matters of national security", according to the Independent Chief Inspector of Borders and Immigration. In 2019, a whistle-blower highlighting a toxic workplace culture at an asylum management unit at the Home Office told the Guardian that employees without security clearance had been accessing the system. It is managed by the Warnings Index Control Unit (WICU) and was in 2015 maintained by Fujitsu.

- "MI5 database": the whistleblower also told the Guardian that staff at the unit had access to an IT system operated by MI5, the UK's domestic intelligence agency, though there is no information available about what this system is, what data it contains, its size, or purpose.

- Semaphore: A database developed by IBM in use since 2004 which compares data from air and other carriers against the Warnings Index for matches, in process of being replaced. In 2019 the Home Office signed a £45m 33-month contract extension with IBM for the system, according to the Register.

- Initial Status Analysis (ISA) database: developed in 2015 as part of the Exit Checks Programme (used to enable to screening of people leaving the UK), it is used to cross check outbound and inbound travel data sent to the Semaphore database by carriers with "data recorded on other Home Office immigration-related systems", in order to check a person's immigration compliance status. It contains "travel histories that consist of an individual's travel in or out of the country, together with data relating to their immigration status, such as periods of leave granted." This includes Advance Passenger Information (API), widely-used passenger data submitted in advance of travel for most scheduled aviation journeys, and Travel Document Information (TDI), passenger data collected at the point of departure for other modes of transport. In addition, it includes data from "case working systems relating to (out-of-country) entry clearance visa application casework and (in-country) casework e.g. on extensions of leave to remain", biometric details submitted prior to visa applications, and passport examinations data collected upon entry into the UK. This data helps mitigate any gaps in inbound API coverage.

B. DATABASES OF RELEVANCE IN DEVELOPMENT

The Home Office is currently developing several large IT systems which will be used to replace existing systems that track individuals throughout the borders, immigration, and customs system and enable the use of surveillance tools by relevant units and officers.

The Department currently manages ten major projects which fall within the "Government Major Projects Portfolio" because they are considered the "largest, most innovative and highest risk projects and programmes delivered by government." Of these, four directly relate to the technological infrastructure underpinning the borders, immigration, and citizenship system:

- Digital Services at the Border (DSAB) / Future Borders and Immigration Systems (FBIS)
- Immigration Platform Technologies (IPT)
- Home Office Biometrics (HOB)
- National Law Enforcement Data Programme (NLEDP)

The National Audit Office concluded in 2018 that the Home Office "has a poor record of delivering IT projects on time and on budget" – and the situation does not appear to have significantly improved.

The Infrastructure and Projects Authority, which oversees the delivery of all major projects across government, carries out an annual review of these projects, grading them with the likelihood of successful delivery and level of associated risks. Ratings are categorised into five groups, which span a range from Red to Green.

In 2020, three of these four projects (DSAB, IPT, & NLEDP) were rated "Amber/Red", meaning that the "Successful delivery of the project is in doubt, with major risks or issues apparent in a number of key areas" requiring urgent action.

Only the Home Office Biometrics programme was rated "Amber", meaning that "Successful delivery appears feasible but significant issues already exist, requiring management attention."

i. Digital Services at the Border (DSAB) / Future Borders and Immigration Systems (FBIS)

Digital Services at the Border (DSAB), a programme within the Digital, Data and Technology unit, aims to build a system to gather data on people and goods coming into and out of the UK and to share that information with the Border Force, police and intelligence agencies.

The aim is to replace a number of obsolete IT systems, including Semaphore. A disastrous 2003 programme known as "e-borders", which was supposed to develop a screening system to analyse data supplied by plane, train and ferry carriers was cancelled by 2015 after the Home Office had spent £830 million on it without delivering large parts of the system.

The Home Office subsequently spent £35 million fighting a legal challenge brought by one of the contractors - US arms company **Raytheon** - which was ultimately awarded £150 million of public money in a settlement with the Home Office.

Having failed to replace the systems, the Home Office then spent an additional £303 million on upgrading the old systems, including Semaphore and the Warnings Index, between 2011-12 and 2014-15, having to rely on them despite them requiring "extensive manual effort" and leading to "duplication of effort", according to the NAO.

Projected to cost some £346 million in total, DSAB is the latest attempt to replace these legacy systems, aiming to "gather and act on data from those people and entities crossing the border, both inbound and out; and provide timely and accurate data to those who need to access/use it." According to tender and contract notices available on the UK government's portal, large tech and arms companies compete for supplying staff and vague services to the programme, but provide little insight as to what the firms are actually supposed to deliver. The programme was supposed to end in 2019.

In 2018, following the UK's decision to leave the EU, the Home Office added more technological requirements to the programme in order to process more data from EU passengers under a programme called the Future Border and Immigration System (FBIS).

In December 2020, the National Audit Office reported that by March 2019 – the end date of DSAB - only an early version of Border Crossing, a system supposed to replace the Warnings Index, was in operation. Two planned systems, supposed to replace Semaphore and a system for tracking freight, had not been realised because of an "expanding scope and lack of clarity over the scope of related projects", including how the Department "would hold data provided by law enforcement and other agencies."

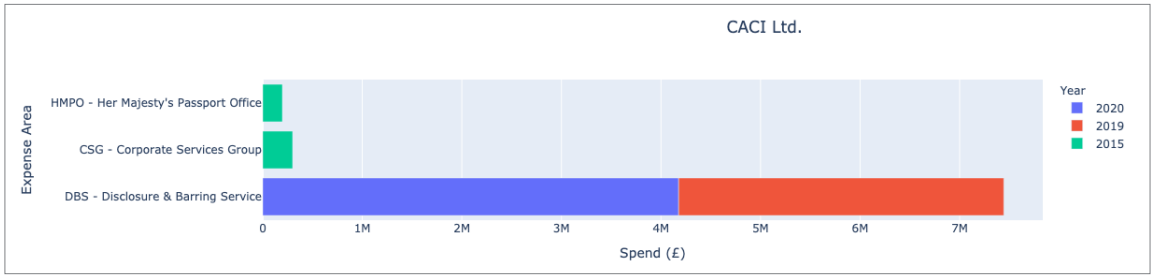
Because of further problems delivering all the systems due to "scope creep and poor programme performance", the National Audit Office noted that a decision to reset the entire programme was taken in 2019 to reduce the scope and push back delivery until 2022.

The NAO concludes that that the estimated "net impact of not delivering to its original timetable of March 2019 is an additional cost of £173 million between 2014-15 and 2021-22."

In 2020, it was announced that £113m has been provided for a newly established Future Borders and Immigration Systems programme, aimed at delivering "a world leading, data driven, digital border" controlling the entry of European Economic Area citizens once free movement ends with Brexit.

Throughout this time, various surveillance and arms companies have won contracts for delivering services under both the DSAB and FBIS programmes.

UK arms firm **BAE Systems** won a £4.9 million contract in 2018, for example, to "supply the capability to deliver discrete work packages aligned to the DSAB programme roadmap", while US security contractor **CACI** won another £4.9 million contract in April 2020 to "deliver a supportable end to end service".

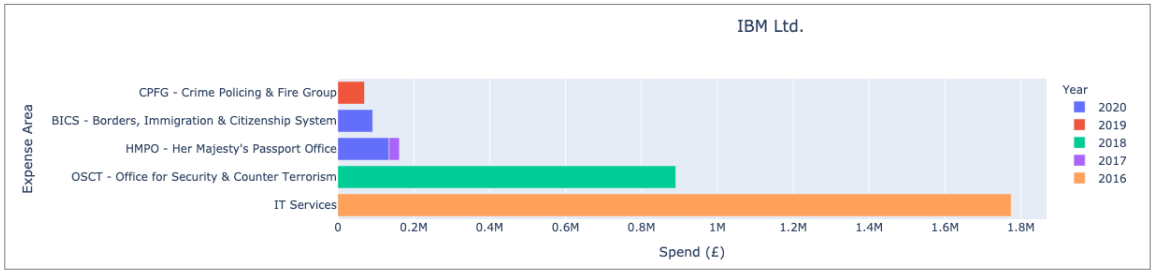


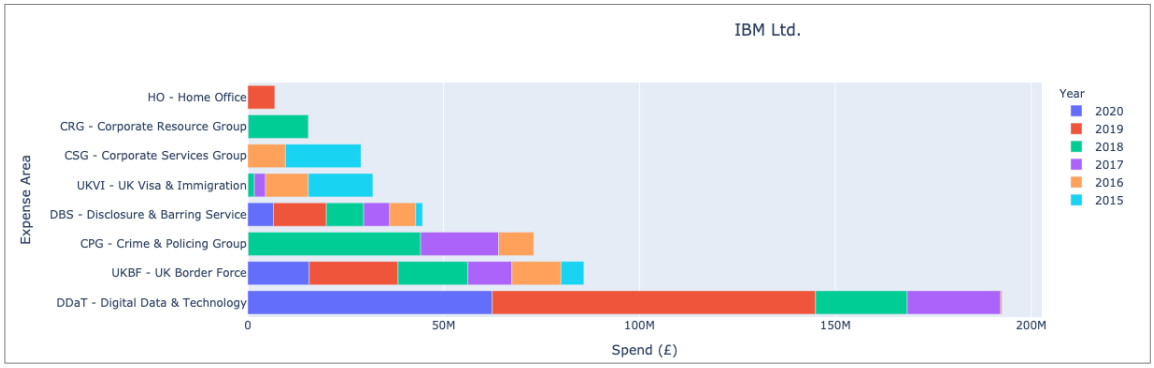
Sum of Home Office expenditure over £25k on CACI, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

US data firm **Teradata** won a £1.78 million contract in 2017 (lasting until 2019) to deliver a "Big Data" capability: a copy of the contract obtained by Privacy International under freedom of information rights similarly provides little insight into the programme and Teradata's role within it.

In 2019, McKinsey & Company were awarded a £1.38 million contract for "scoping, planning and initial delivery" of the FBIS programme under a single tender, while UK-based AHE Partnership were awarded a £230,000 in October 2020 for planning and other services.

Because of the failure to deliver the programme by 2019, as reported by the Register, the Home Office signed a £45 million contract with **IBM** in 2019 to extend the use of Semaphore.





Sum of Home Office expenditure over £25k on IBM, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

In addition to these programmes at the Home Office, in September 2020 the Guardian reported that a borders unit at the Cabinet Office had awarded **Palantir**, a US surveillance firm notorious for contracting with the Immigration and Customs Enforcement (ICE) agency in the US, a contract to "monitor any potential impacts resulting from border controls being imposed by EU member states on goods or people coming from the UK."

A contract notice later published by the Government states that Palantir will provide the services in two phases. Phase one involves scoping the technical feasibility of using data and metadata from border databases across government departments and commercial third parties and integrating them into Palantir's Foundry software. This "Border Flow Tool" is aimed at providing "a situational awareness capability at the border… through the means of analytical reporting and data visualisation".

While phase one will be provided "for free", if Palantir believes that its Foundry system can successfully provide such a service, it will integrate all the datasets for a fee of just under £14 million.

An internal Home Office document noted that data from Home Office systems will be provided to Palantir and that the Home Office was required to deliver the technical integration by the end of November, though it is not known what exact data Palantir is likely to have access to or integrate into its platform. PI recently co-authored with NoTech4Tyrants a review of how the data analytics company has embedded itself throughout the UK.

ii. Immigration Platform Technologies

Immigration Platform Technologies (IPT) aims to build a platform to manage immigration, visa, and asylum applications and casework. The £250 million project, which began in 2014 and has delivered some functions, is supposed to replace existing databases, including the Case Information Database, the Asylum Support System, and the Biometric Residence Permit system.

A previous attempt at replacing the Case Information Database (CID) and other older systems, under a programme called Immigration Case Work (ICW), was closed in 2013 having "having achieved much less than planned", according to the NAO. Despite spending £347 million on the system, staff were subsequently left relying on paper systems and the CID, which according to the NAO was error-prone and had a "history of systems freezing and being unusable".

In 2019, it was revealed that some 98% of staff working on the programme are temporary staff; Accenture, 6Point6, Atos, Deloitte Digital, Capgemini, IBM, PA Consulting, Mastek, BJSS, and Cognizant are all listed as some of the main suppliers to the project.

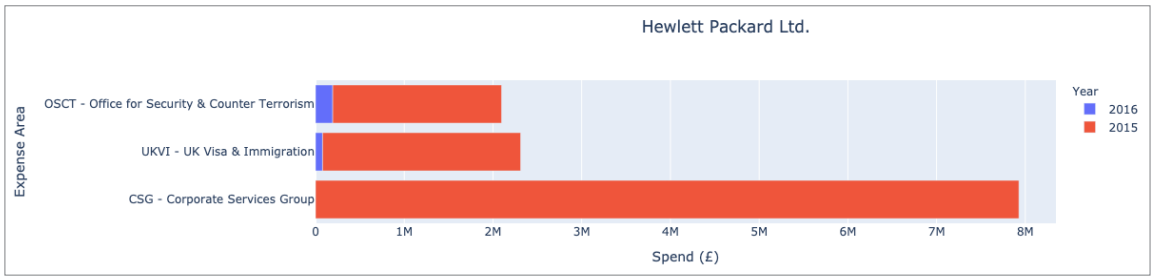
In 2014, several companies were hired to develop systems aimed at replacing parts of ASYS, the Biometric Residence Permit system, and the asylum functionality of the Casework Information Database.

A project called "Biometric Residence Permit Total" initiated in 2014 by the unit aimed to provide the foundations for the capability to allow government

departments and other "users" to cross-check people's immigration status using their biometrics. Three suppliers were contracted to provide the foundations for such a system, by developing an interface between biometric capture systems and a range of internal and external systems which would "provide the initial interfaces to calculate immigration status, beginning with those migrants issued with a BRP and making this information available to relevant users".

Another project within the tender sought to provide a new case management system for the Asylum Casework Directorate, enabling it to do things like create new records, access files, and then refer people denied asylum to Immigration Enforcement, as well as manage the provision of support to asylum seekers.

Under the tender, HP Enterprises was awarded a contract (estimated to be worth £2.7 million), as well as two smaller UK-based companies, Agilesphere (£437,000) and Transform Innovation (£650,000). Transform Innovation was itself dissolved in 2015 however, and it is not known whether the core functionalities were delivered.



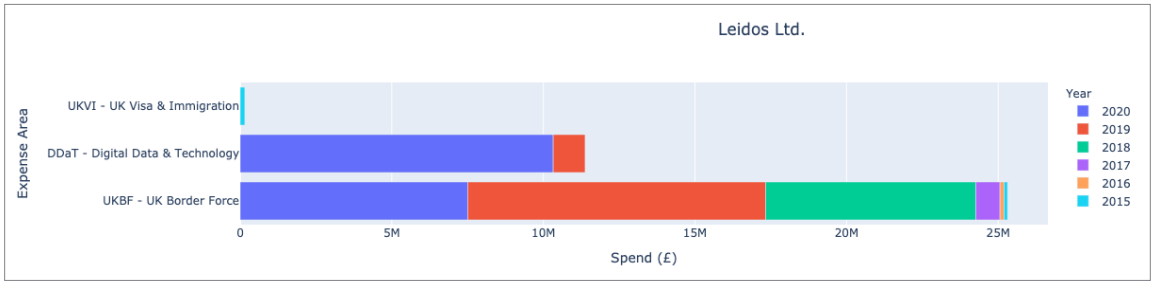
Sum of Home Office expenditure over £25k on HP, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

iii. Home Office Biometrics (HOB)

The Home Office Biometrics Programme (HOB) wants to maximise "the public safety benefits of fingerprints, DNA and facial matching" by transforming "the existing siloed biometrics capabilities into a technically converged, but commercially disaggregated, strategic biometrics capability." In effect, it wants to merge existing sources of biometric data and make them more readily available to more users. The databases that will be converged comprise The National DNA Database, The Immigration and Asylum Biometric System (IABS), and the Law Enforcement and Security Biometrics System (IDENT1).

By converging facial, DNA, and fingerprint data into a single platform, biometric data will be more easily available to more agencies.

HOB has awarded **Leidos**, a US tech company, a contract valued at £300 million to among other things merge the IABS and IDENT1 systems onto a single platform.



Sum of Home Office expenditure over £25k on Leidos, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

iv. National Law Enforcement Data Programme (NLEDP)

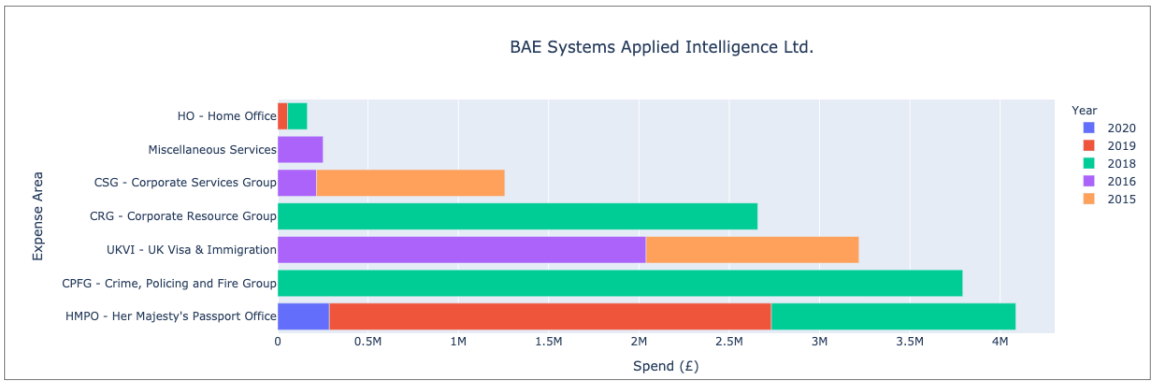
The Home Office National Law Enforcement Data Programme (NLEDP) is separate from HOB, though their objectives and operations significantly overlap. NLEDP is currently in charge of developing the Law Enforcement Data Service (LEDS), a new "mega-database" to be used by police and other government agencies.

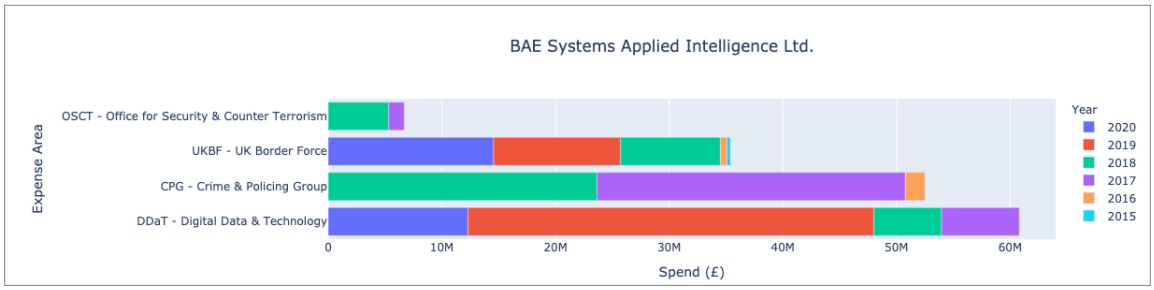
LEDS is a new platform, which will replace and combine the existing Police National Database (PND) and the Police National Computer (PNC) – two of the main databases used by police for accessing evidence and intelligence. The Home Office expects the first stage of LEDS to be operational by late 2020 and will continue to add further data sources through to 2023 and beyond.

How it will interplay generally with immigration data and agencies is yet to be determined. Privacy International understands that this is still being decided through engagement between the Home Office, police, and immigration authorities: we are calling for appropriate technical and legal safeguards to be put in place to ensure that LEDS is not used for immigration enforcement.

ADS, the UK's main arms lobby group, have an "Industry Reference Group" with the NLEDP whereby they engage with the programme by "receiving updates on the status of the Programme", "providing feedback to NLEDP on the evolving business and technical architectures", and "developing think pieces for the Programme team to consider". Privacy International and other civil society groups are also engaging with the Home Office on the development of the programme, aiming to better understand the threats posed to people's rights and how they can be mitigated.

BAE Systems were awarded a £14 million contract in 2016, and IBM were awarded a £12 million contract in 2017 for development of LEDS.


BAE Systems Applied Intelligence Ltd.
Expense Area
HO - Home Office
Miscellaneous Services
CSG - Corporate Services Group
CRG - Corporate Resource Group
UKVI - UK Visa & Immigration
CPFG - Crime, Policing and Fire Group
HMPO - Her Majesty's Passport Office
0
0.5M
1M
1.5M
2M
2.5M
3M
3.5M
4M
Spend (£)
Year
2020
2019
2018
2016
2015


BAE Systems Applied Intelligence Ltd.
Expense Area
OSCT - Office for Security & Counter Terrorism
UKBF - UK Border Force
CPG - Crime & Policing Group
DDaT - Digital Data & Technology
0
10M
20M
30M
40M
50M
60M
Spend (£)
Year
2020
2019
2018
2017
2016
2015

3. "FRONT-END" TOOLS

KEY FINDINGS

- The convergence of datasets and their increased availability to new agencies enabled by mobile biometric scanning devices has empowered police and immigration enforcement officers to rapidly identify people and check their immigration status.

- The Digital, Data and Technology unit is developing a system known internally as the 'Status Checking' Project aimed at obtaining and sharing "an individual's immigration status in real time with authorised users, providing proof of entitlement to a range of public and private services, such as work, rented accommodation, healthcare and benefits."

- Border entry points and the sea are monitored by the Border Force and other authorities, with several private companies providing technology.

Many of these "back-end" systems can and are being used to facilitate the surveillance and tracking of people by other systems and frontline officers.

Other surveillance tools available to authorities have no connection to these "back-end" databases, and are also described below.

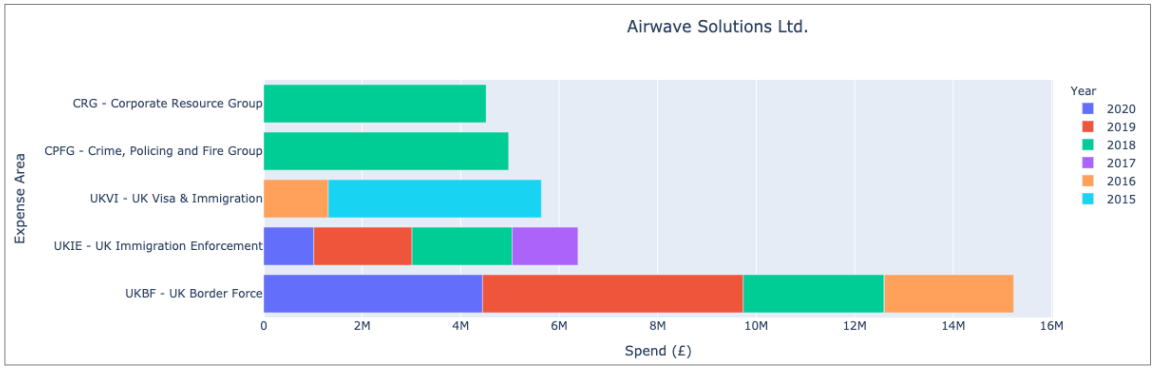
A. MOBILE SCANNERS

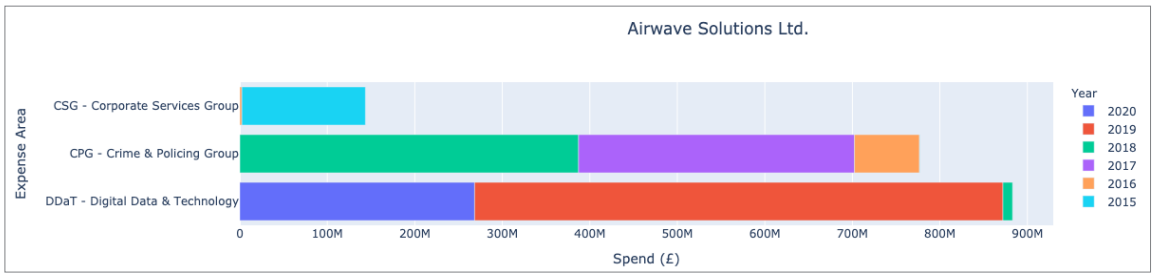
The convergence of these datasets by HOB and the NLEDP has already had important implications. By increasing availability of data to new agencies, it has empowered police and immigration enforcement officers equipped with mobile biometric scanning devices to rapidly identify people and check their immigration status.

According to HOB, if an officer suspects someone of committing an offence and providing false information about their identity, they can take fingerprints from them - even if they are not being arrested, and without their consent.

Twenty-one forces are currently using mobile fingerprint systems connected to a vast pool of data on IABS, IDENT1 and police databases, according to British arms company BAE Systems, which credits itself for developing the backend interface.

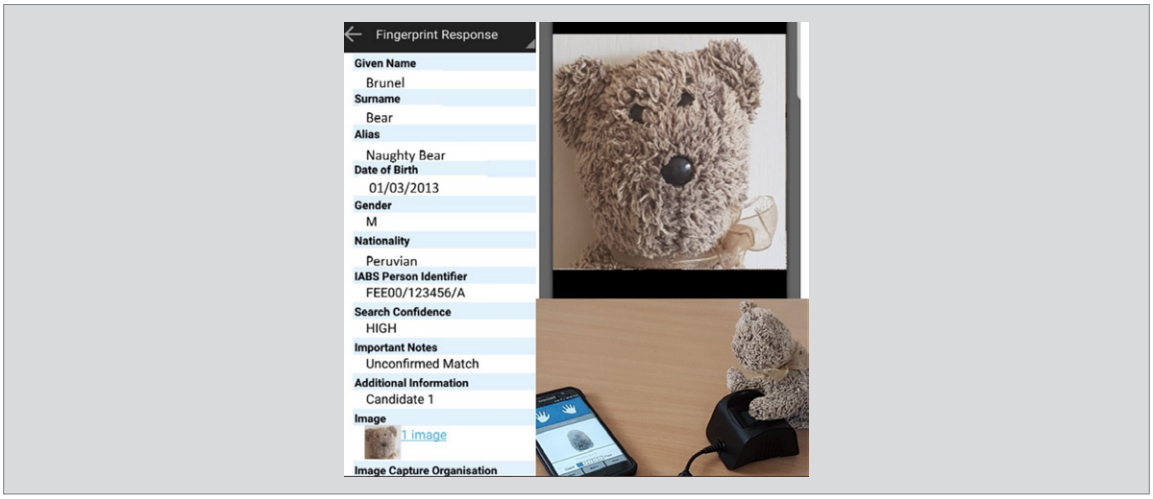
Immigration Enforcement officers also have access to the databases on handsets provided by **Airwave Solution Ltd**, which has received £4.36m in payments from Immigration Enforcement since 2017, according to government expenditure data.

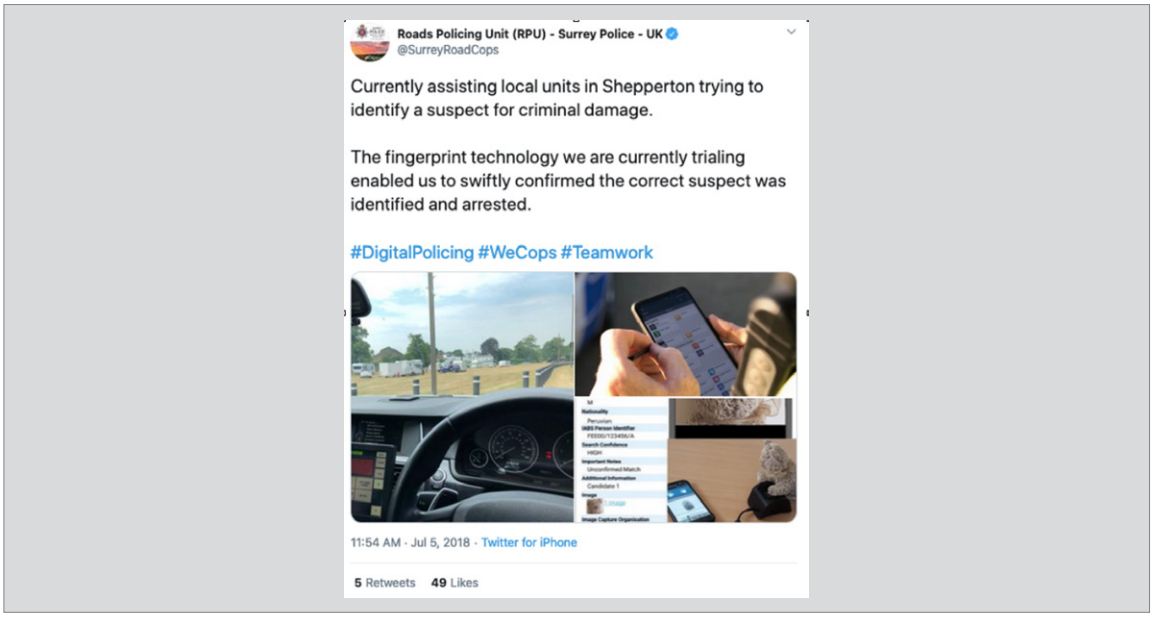




Sum of Home Office expenditure over £25k on Airwave, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

West Yorkshire Police's policy on the scanners states that *"Should officers identify that the individual stopped and checked via mobile identification and the data returned indicates they are a person of interest to Home Office Immigration Enforcement then contact* **must** *[original emphasis] be made immediately with the Command and Control Unit (CCU)."* The policy further states that *"immigration database will not routinely be checked, there must be grounds for suggesting that the suspect is an immigration offender before both databases are checked".*





Screenshots taken from Surrey Police's Twitter account showing a mock-up of the data available through the biometric scanners, including IABS data

Providing officers such instant access incentivises officers to run discriminatory immigration checks on people. People perceived by officers as "non-British" can be targeted, and such officers will be empowered to run instant immigration status checks on people: this clearly enables further discrimination against people who are not white, or who do not speak with a 'British' accent'.

In addition, this may deter people with irregular status from speaking to officers, including victims of crime. Liberty reports that in 2017 a pregnant woman who had been repeatedly raped was subsequently arrested at a rape crisis centre on immigration grounds.

While the main biometric data is currently fingerprints, the programme will expand to other forms. HOB also aims to build a "biometric search, identification and verification" capability for facial images, including a new algorithm to allow law enforcement to carry out facial image matching, meaning that similar immigration checks could be conducted through facial recognition technology.

This in turn might mean more racial discrimination: it's been widely reported misidentification errors disproportionately affect minority groups, who as a result are then likely to be wrongly stopped and questioned. For example, past facial recognition trials in London resulted in an error rate greater than 95 per cent, leading even to a 14-year-old black schoolboy being "fingerprinted after being misidentified".

B. "STATUS CHECKING"

The Digital, Data and Technology unit is developing a system known internally as the 'Status Checking' Project aimed at obtaining and sharing "an individual's immigration status in real time with authorised users, providing proof of entitlement to a range of public and private services, such as work, rented accommodation, healthcare and benefits."

For example, by using "APIs" – methods of communicating between computer programmes – in this case connecting to the "back-end" databases, landlords would be able to check a person's immigration status, for example by checking whether they hold a Biometric Residence Permit.

Building on the capabilities under the Biometric Residence Permit Total project, described above, the Home Office envisaged in 2014 developing an "Enhanced Search and Data Sharing service" which "exposes the information held in the immigration caseworking systems (in a secure manner) to allow for biometric cross checking by other departments, most notably immigration enforcement and the Police, and for the Home Office to exchange data with other members of the Five Country Conference (FCC) in order to combat crime and terrorism."

C. BORDER SURVEILLANCE

Border entry points and the sea are monitored by the Border Force and other authorities, with several private companies providing technology.

Last January, drones provided by Portuguese arms company **Tekever** were first reported by Wired to be flying over the Channel, likely looking for migrants on boats. Tekever and the Home Office's Border Force are both part of a research project using "manned and unmanned technologies and tools, both of aerial and underwater coverage" for maritime surveillance. The project's nearly €6 million budget is funded by the Union, as part of an increasingly securitized European research agenda which gives millions to the security industry to develop new tools of surveillance .

Israeli defence company **Elbit** was awarded a contract worth nearly £1 million to test a drone system for the UK's Maritime and Coastguard Agency in February 2020, something it also does for the EU in the Mediterranean and for Israeli authorities monitoring people in Gaza, according to the Euro-Mediterranean Human Rights Monitor. Elbit also sells a range of electronic surveillance tech, including spyware used to target people's devices and which has been reported by Citizen Lab to be used against Ethiopian dissidents, including in the UK.

On land, the Border Force uses a combination of cameras, security guards, sniffer dogs, x-ray monitors, motion sensors, carbon dioxide detectors (to detect people's breathe), and heartrate monitors to identify people in vehicles.

UK-based manufacturer of heartbeat monitors Clantect **Ltd** received over £1.4 million in payments from the Border Force in 2017-18, while US seller of cargo and vehicle inspection tech Rapiscan received just under £1.7 million since 2015.



Brochure of Clantect Heartbeat Monitor

D. LANGUAGE ANALYSIS

If a Home Office caseworker doubts an asylum seeker's claim to be from a certain place, they can hire an external company to assess their language and provide their opinion as to where they might be from. But rather than interpreters, since 2014, the Home Office has used two Swedish companies, Verified AB and Spraklab to run tests on asylum seekers.

In 2019, the Guardian revealed that 2 in 5 Syrian asylum seekers were subject to the testing, and that 5900 such tests had been carried out between 2011 and 2018, including on people who already had reliable documents. In one case, the Guardian found that the author of a report which was used to dispute the nationality of a Syrian asylum seeker could not themselves speak Arabic.

E. MOBILE PHONE EXTRACTION

Mobile phones are important to everyone, but as a vital source of safety information for asylum seekers they can mean life or death. However, surveillance companies and border authorities also target them as a source of intelligence by connecting them to surveillance software, through a process known as mobile phone extraction.

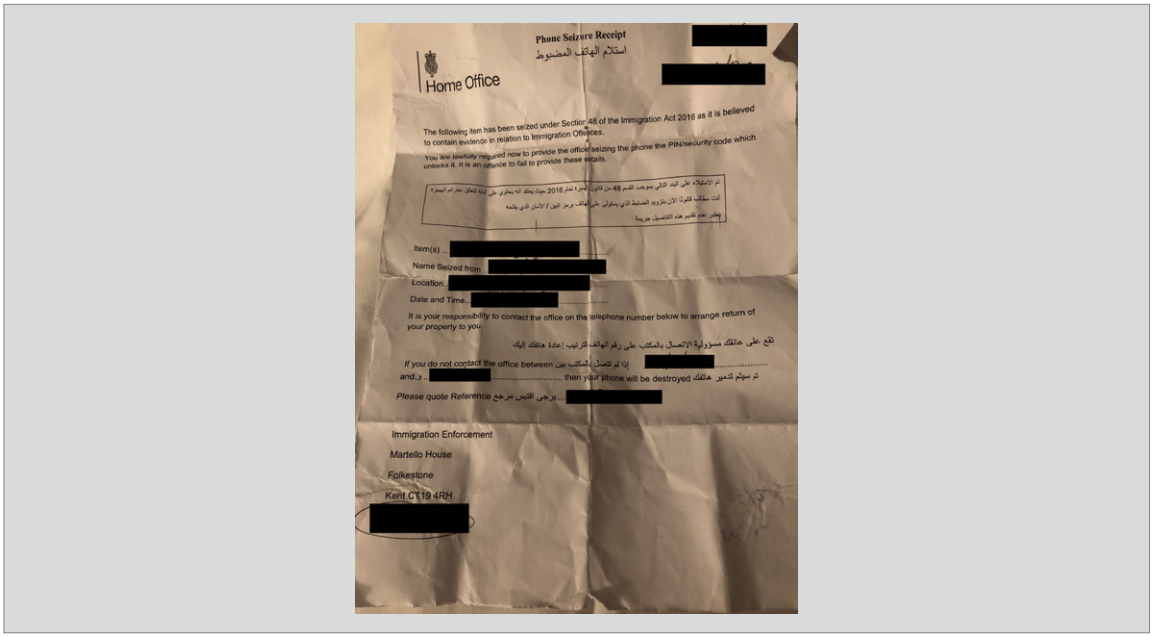
Israeli-based surveillance company Cellebrite, for example, explicitly markets its software used to extract a device's data to authorities interrogating asylum seekers' applications.

By analysing the phone, Cellebrite claims its technology can audit a "person's journey to identify suspicious activity prior to arrival", track their route, run a keyword and image search through their device to identify "traces of illicit activity", and review their online browsing and social media activity.

Location tracking is performed by accessing GPS records on the device, as well as phone metadata (which could, for example, be the location information automatically associated with photos and networks to which the device has connected) and locations based on social media posts.

Once the device is accessed, the software also analyses data stored on the cloud – which typically includes back-ups of files. An analysis of Cellebrite's software conducted by Privacy International found that it could retrieve data which the user may believe has been deleted.

In 2018, the UK Border Force and Immigration Enforcement made payments of £133,000 to Cellebrite, while the Border Force, Immigration Enforcement, and UKVI paid £335,000 to Micro Systemation, a similar extraction company based in Sweden.



Phone Seizure Receipt

استلام الهاتف المضبوط

Home Office

The following item has been seized under Section 48 of the Immigration Act 2016 as it is believed to contain evidence in relation to Immigration Offences.

You are lawfully required now to provide the officer seizing the phone the PIN/security code which unlocks it. It is an offence to fail to provide these details.

Item(s)

Name Seized from

Location

Date and Time

It is your responsibility to contact the office on the telephone number below to arrange return of your property to you.

If you do not contact the office between ... and ... then your phone will be destroyed

Please quote Reference

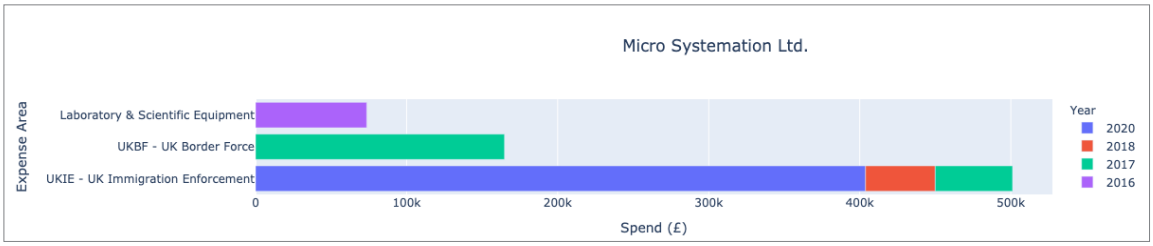
Immigration Enforcement

Marteilo House

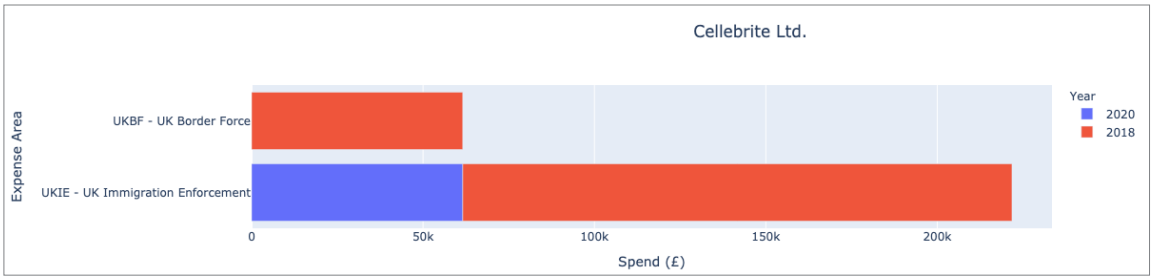
Folkestone

Kent CT19 4RH

Example provided to Privacy International of a phone seizure notice given to people by Immigration Enforcement



Sum of Home Office expenditure over £25k on Micro Systemation, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.



Sum of Home Office expenditure over £25k on Cellebrite, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

F. HACKING

UK immigration authorities also have 'equipment interference' powers under the Investigatory Powers Act, which means they are able to do things like hack into devices or networks to extract information or track its activities in real time. State hacking is one of the most intrusive forms of surveillance, allowing authorities access to everything on a person's device as well as the ability to take control of functions such as the webcam and camera.

Under the Investigatory Powers Act 2016, a senior immigration official may issue a warrant for targeted equipment interference "for the purpose of preventing or detecting serious crime" related to an immigration or nationality offence, which must then be approved by a Judicial Commissioner.

The Guardian reports that a document detailing the hacking powers available to immigration officers claimed it "is to ensure that immigration officers can deploy a full range of investigative techniques to deal effectively with all immigration crime".

It is not known how many equipment interference warrants have been sought or granted for use by immigrations officials.

G. WI-FI ANALYSIS

The Covert Investigation Team at Immigration Enforcement provide technical support to investigations at the department. In 2017 they contracted **3gforensics**, a UK surveillance company, to provide "MacGrabber", a tool which it markets as "Information collection and analysis for the modern age".

The contract award, worth £17,230, specifies that MacGrabber is for the "capture and analysis of Wi-Fi traffic data", enabling investigators to gather intelligence from "organised crime groups who are routinely using Wi-Fi".

H. COMMUNICATIONS DATA SURVEILLANCE

Over 500 public authorities in the UK are able to request that telecommunications operators provide what is known as Communications Data – the 'who, what, when, and how' of communications. Communications Data includes information about websites a device has accessed, as well as the location of a device if it is known.

In 2018, Immigration Enforcement received 7,297 pieces of Communications Data, a slight decrease from 7,770 in 2017.

I. SURVEILLANCE VANS

In 2014, Immigration Enforcement signed a contract worth nearly £300,000 with 'S. MacNeillie & Son Ltd', now Babcock International Group, to equip a fleet of cars, vans and motorcycles with surveillance cameras. The surveillance vans are equipped with cameras concealed within car headrests and "housed within baby seat concealments".

The contract also included the provision of "long range cameras capable of being stationed within an unmanned observation post with remote access from an Immigration Enforcement staffed operations room", as well as the ability to read license plates from 1000m using Automatic Number Plate Recognition (ANPR) technology.

Immigration Enforcement also paid the vehicle engineering arm of Babcock over £1.25m in 2017, according to Home Office spending data.

J. SATELLITE TRACKING

Where a person is subject to 'immigration bail' under Schedule 10 of the Immigration Act 2016, the Home Office can use electronic tagging technology to monitor their movements. In 2016, the Home Office told the Independent Chief Inspector of Borders and Immigration that some 360 foreign nationals were currently tagged, and that its intention was to tag all foreign national offenders, except those under 18.

In 2017, the Immigration Enforcement released a tender for a satellite tracking device that would continuously track someone and alert them if they were to take it off.

K. INTELLIGENCE SHARING SOFTWARE

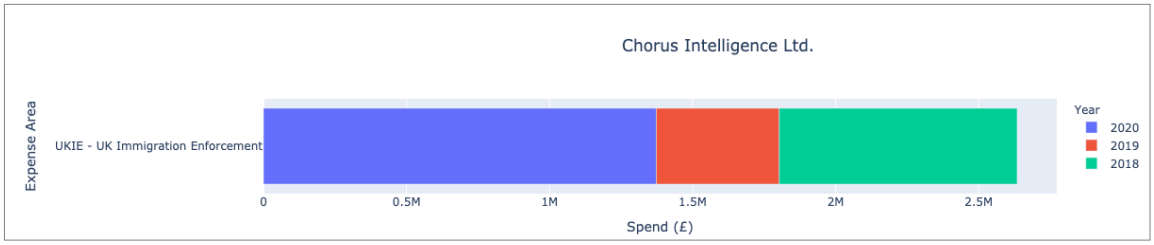
Immigration Enforcement, Border Force, and the Passport Office use intelligence sharing software called the Single Intelligence Platform (SIP) which went online in 2016. The software centralised 16 different data sources and now provides a "single, consistent platform for Home Office staff to collect, check, share and access myriad intelligence data" across the agencies.

Equal Experts, a software company, was awarded a contract in 2016 for £1.22 million for replacing the prior system, and graph software which allows users to visualise any collected intelligence is provided by Neo4j at a cost of £520,000.

L. DATA ANALYTICS

Once an agency obtains data from devices, telecommunications operators, or companies, they can use software which claims to be able to cleanse, analyse and visualise it. Others claim to be able to use it for making predictions about future events or behaviour. While many of the claims of this industry are likely to be highly exaggerated, the marketing promises much.

For example, UK data company Chorus Intelligence, which received £684,552 in payments from Immigration Enforcement in 2018, claims that one of its products is able to find "previously hidden connections and [open] up new lines of enquiry, putting actionable intelligence in the hands of Investigators *fast*."



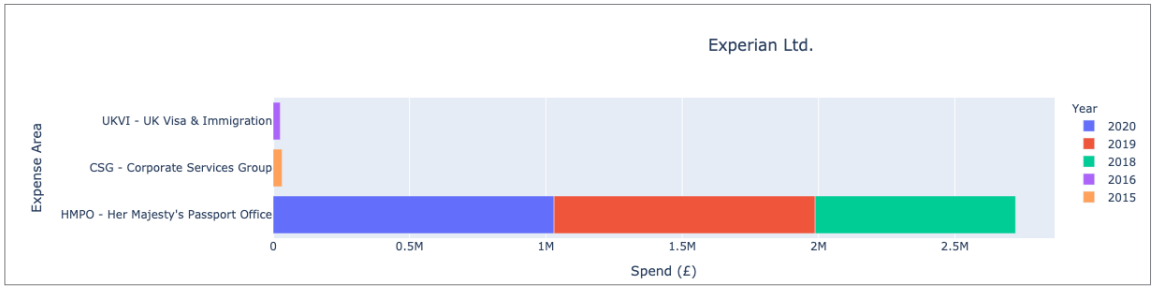
Sum of Home Office expenditure over £25k on Chorus Intelligence, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

US Basis Technology, which received a £46,880 payment from the Border Force in 2018, claims to use 'AI' to discover intelligence by analysing text, for example identifying people and their history on social media in other languages, such as Arabic, so that border officers can question them.

M. DATA BROKERS

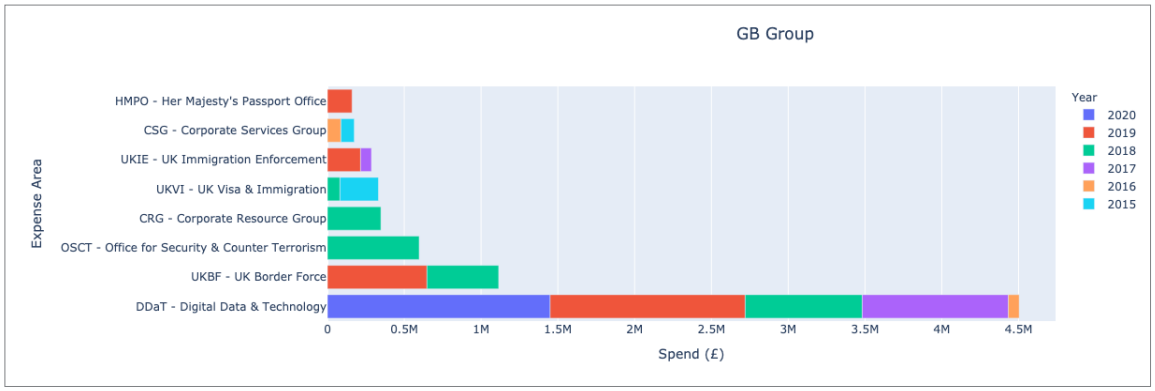
Data brokers are opaque companies you may never have heard of who collect and trade data for profit, including huge credit agencies which trade on the information of millions of people and build intricate profiles about our lives. Privacy International has filed complaints with authorities in France, the UK, and Ireland for wide-scale and systematic infringements of data protection law by the data broker industry.

In response to a parliamentary question in 2018, the UK government confirmed that it contracts Experian – one of the UK's leading credit reference agencies – to conduct financial checks for immigration purposes. An undated manual for Immigration Enforcement officers also says that in addition to Experian, Intelligence Units also conduct checks using "GB Accelerator", a contact database sold as a tool for locating missing customers by GB Group, a data broker.



Sum of Home Office expenditure over £25k on Experian, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

GB Group, which markets itself as "the global technology specialist in fraud, location and identity data intelligence" with the "Ability to verify billions people in over 70 countries, ~60% of world population" has received £3.7m in payments from the Home Office since 2015, including by Immigration Enforcement and the Border Force.



Sum of Home Office expenditure over £25k on GB Group, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

4. INTERNATIONAL OPERATIONS

KEY FACTS

- Fingerprints of asylum seekers are searched against the main criminal fingerprinting database used by law enforcement in the UK, the IDENT1. They are also run against the databases of other countries, providing authorities with access to any information associated with those prints, including the EURODAC - a pan-European asylum fingerprint database containing more than 7 million records.

- Under "Project Hunter", the UK Border Force uses aid money to bolster the "border intelligence and targeting" capabilities of foreign security agencies with UK know-how and equipment. The Border Force is also advising countries on amending legislation to facilitate data gathering and targeting, as well as providing data analysis services.

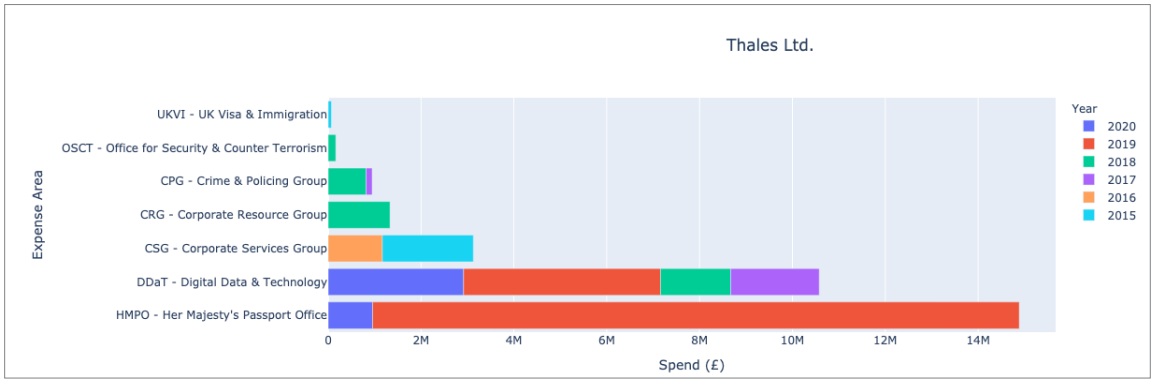
- The UK intelligence agencies, together with counterparts in Australia, Canada, New Zealand, and the US, are part of an intelligence alliance called the "Five Eyes" through which they coordinate intelligence collection, operations, and sharing. There is also an equivalent for immigration agencies, called the Five Country Conference.

As well as running a vast domestic tracking and surveillance system, UK immigration authorities also work with international counterparts to increase their surveillance capabilities.

A. INTERNATIONAL BIOMETRIC DATA SHARING

As well as running the fingerprints of asylum seekers collected by UKVI against the IDENT1, they are also run against the databases of other countries, providing authorities with access to any information associated with those prints.

For example, fingerprints of asylum seekers collected when they make an application are also checked against the EURODAC - a pan-European asylum fingerprint database containing more than 7 million records (a core part of which is provided by European arms company **Thales**).

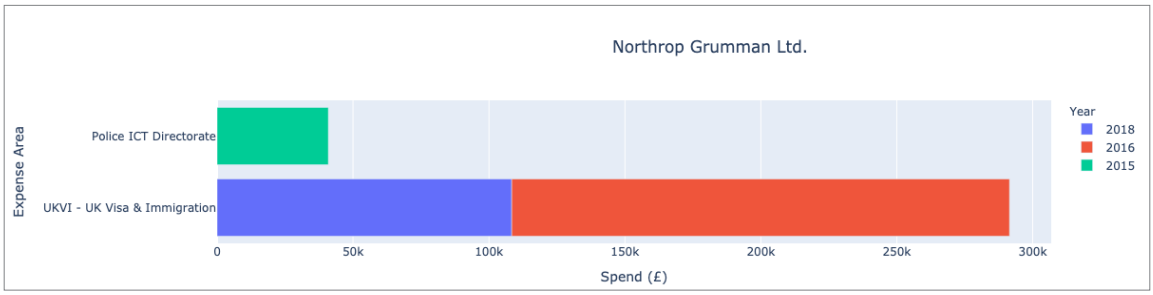


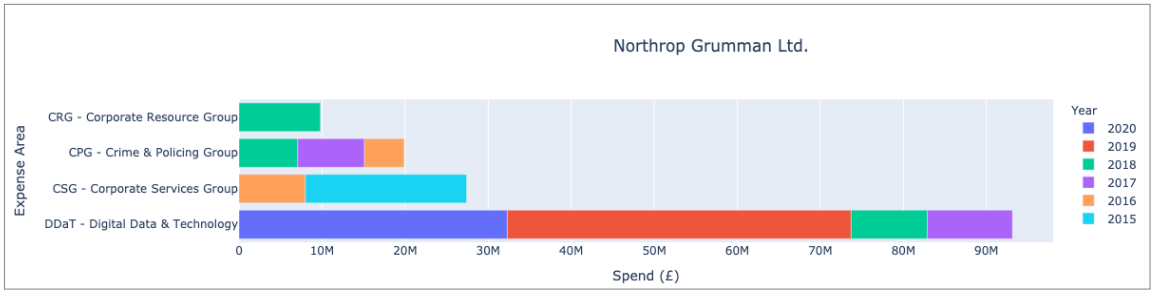
Sum of Home Office expenditure over £25k on Thales, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

The UK intelligence agencies, together with counterparts in Australia, Canada, New Zealand, and the US, are part of an intelligence alliance called the "Five Eyes" through which they coordinate intelligence collection, operations, and sharing. There is also an equivalent for immigration agencies, called the Five Country Conference, through which significant data-sharing is conducted.

Under the Five Country Conference (FCC) Data-Sharing Protocol agreed in 2009, these countries share the biometric records of (initially) up to three thousand asylum seekers with one another per year as well as any information associated with that print. This information can then be stored on the applicant's Case Information Database, and any adverse or contradictory information can be used against people in their claim.

Such data and requests for UK data may come from the US Department of Homeland Security (DHS) biometric system, known as IDENT (not to be confused with the UK's IDENT1). It is currently being replaced by HART, also developed by **Northrop Grumman**, and will scoop up a whopping 180 million new biometric transactions per year by 2022. Once a match is made, authorities may "further collaborate and review the match by exchanging additional information allowable under applicable law to determine whether further action is required using other existing protocols (law enforcement or otherwise) between the countries."





Sum of Home Office expenditure over £25k on Northrop Grumman, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

B. SURVEILLANCE OUTSOURCING

Border Force and Immigration Enforcement both have staff in international locations and work with foreign agencies to ensure they can carry out surveillance.

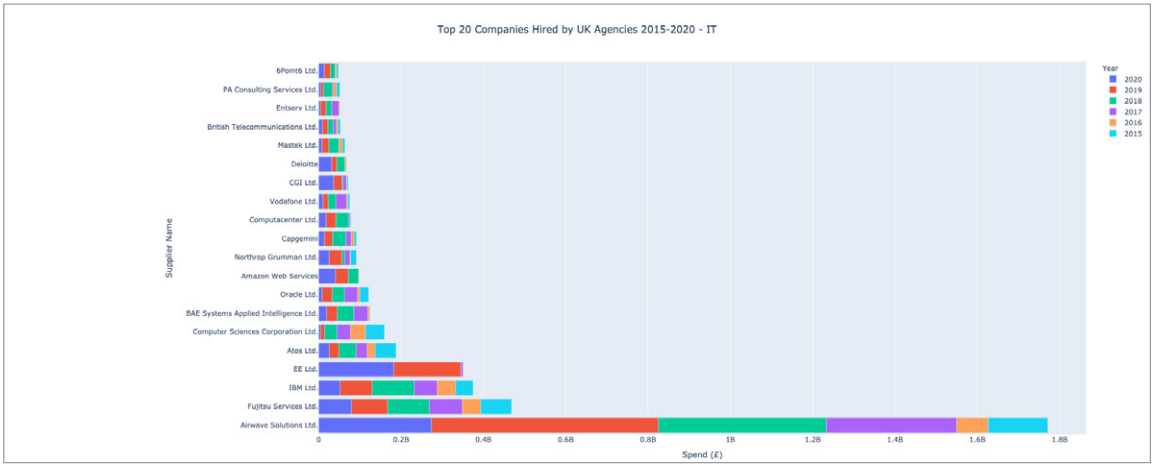
Under "Project Hunter", the UK Border Force uses aid money to bolster the "border intelligence and targeting" capabilities of foreign security agencies with UK know-how and equipment.

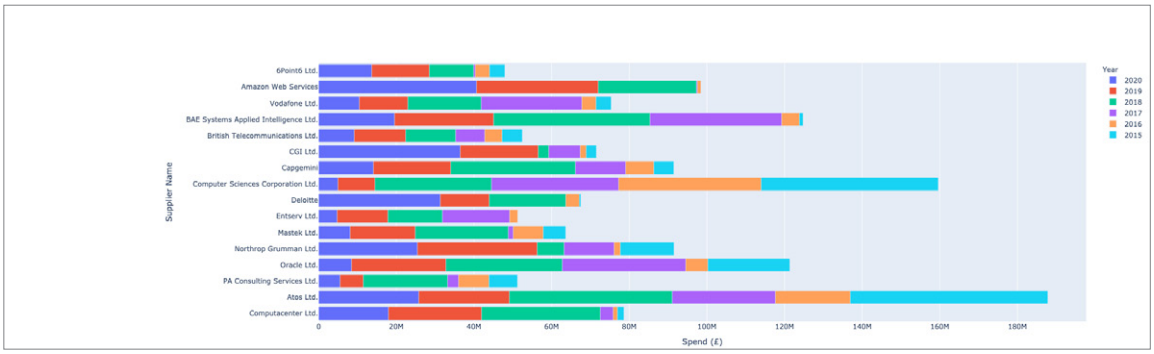
As well as the provision of equipment and training, the Border Force is also advising countries on amending legislation to facilitate data gathering and targeting, as well as providing data analysis services.

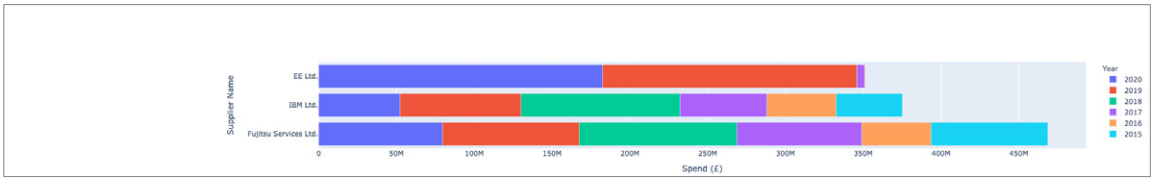
Similarly, the Home Office's Immigration Enforcement arm uses aid money to train authorities and provide equipment aimed at stopping irregular migration through, for example, training in forgery detection, passenger profiling and by providing associated equipment, such as portable evidence recorders. Immigration Enforcement International also has staff at embassies responsible for developing intelligence and investigations for use in the UK and where they are stationed. In 2019/20, the unit trained 7000 people, including in things like open source techniques, arrest training, and investigation skills, and carried out work in 39 countries.

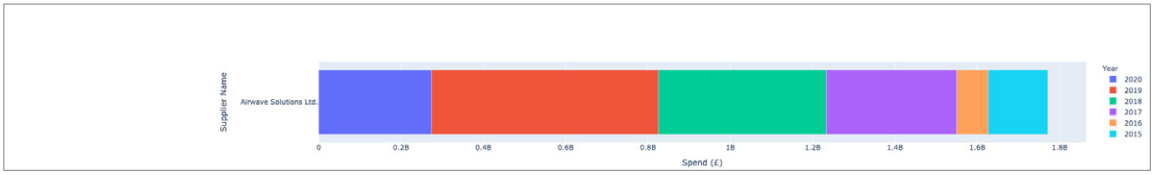
In 2019, Immigration Enforcement International contracted Mobile Content Management Solutions to provide 2 laptops and unknown software for £47,654. UK-based Mobile Content Management Solutions, which has on its board a former Parliamentary Under-Secretary of State at the Home Office, describes itself as the creator of a digital forensics platform used to acquire and analyse data from devices.

This is part of a broader trend of countries such as the UK, US, and across the EU bolstering foreign security agencies to stop migration and gain access to data and intelligence on foreign populations for migration control purposes.









Sum of Home Office expenditure over £25k on select suppliers listed under "IT" categories, 2015 - 2020. Sums based on data available from https://www.gov.uk/government/publications/home-office-spending-over-25000-2020 and previous years.

5. RESEARCH RESOURCES

Further information regarding the UK's borders, immigration, and citizenship system, surveillance powers, and procurement can be found in government and non-government sources.

GOVERNMENT

- https://www.gov.uk/contracts-finder
  A platform for searching published contracts

- https://www.gov.uk/government/publications/home-office-spending-over-25000-2020
  A source of individual payments made by the Department

- https://devtracker.fcdo.gov.uk/

  A searchable platform describing UK development aid projects

- https://www.blpd.gov.uk

  A procurement site for UK emergency services

- https://ipco.org.uk/

  Investigatory Powers Commissioner's Office, the main oversight body for the use of investigatory powers by UK agencies, including annuals reports

NON-GOVERNMENTAL

- https://www.thebureauinvestigates.com/stories/2019-05-08/algorithms-government-it-systems

  A report detailing public expenditure by the Home Office produced by the Bureau for Investigative Journalism

- https://privacyinternational.org/long-read/2225/open-source-guide-researching-surveillance-transfers

  A guide for finding out which surveillance equipment has been exported to where globally

- https://privacyinternational.org/long-read/993/guide-international-law-and-surveillance-20

  A detailed reference tool describing substantive articulations of law regarding surveillance

- https://medium.com/@mary.atkinson.123/lets-talk-about-the-costs-of-borders-c98e7cbc7d91

  A review of Home Office procurement for immigration enforcement

- https://www.statewatch.org/publications/

  Multiple reports describing EU information systems and immigration databases

- https://www.statewatch.org/news/2020/september/eu-study-on-the-political-economy-of-border-control-measures/

  EU Horizon-funded report summarizing "the "political economy of entry governance", including an analysis of contracts and lobbying efforts.

6. LIST OF COMPANIES MENTIONED IN THE GUIDE

- Accenture
- Agilesphere
- Airwave Solution Ltd
- Atos
- BAE Systems
- Babcock International Group
- BJSS
- CACI
- Capgemini
- Cellebrite
- Chorus Intelligence
- Clantect Ltd
- Cognizant
- Deloitte Digital
- Elbit Systems
- Equal Experts
- Experian
- Fujitsu
- GB Group
- HP Enterprises
- IBM
- LEIDOS
- Mastek
- Microsystemation
- Mobile Content Management Solutions
- Northrop Grumman
- PA Consulting
- Palantir
- Rapiscan
- Raytheon
- Spraklab
- Tekever
- Teradata
- Thales
- Transform Innovation
- US Basis Technology
- Verified AB
- 3gforensics
- 6Point6

This report was finalised in November 2020.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).