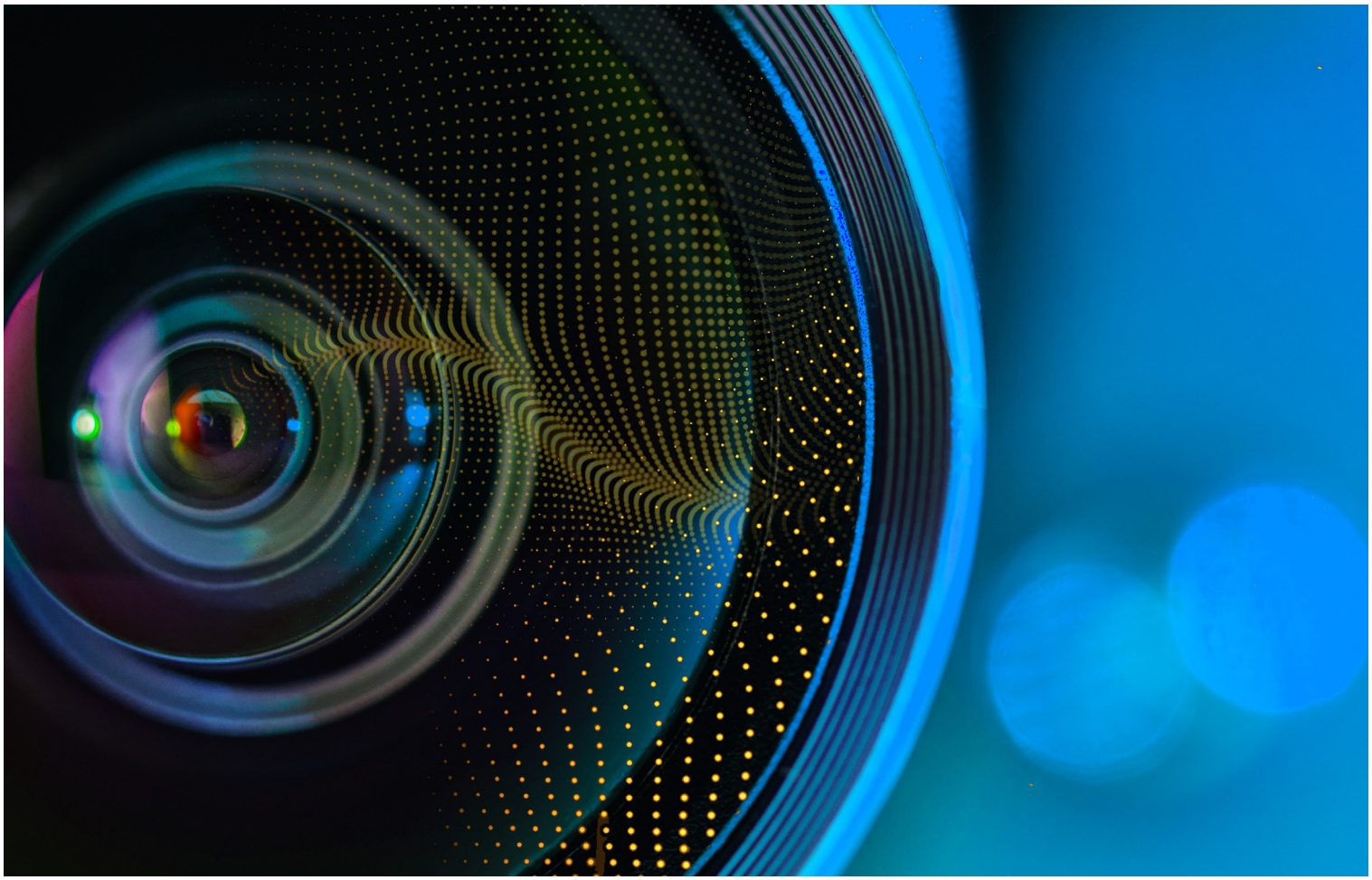
Oxford Commission on AI & Good Governance

OXFORD INTERNET INSTITUTE

UNIVERSITY OF OXFORD



Surveillance as a Service

The European AI-Assisted Mass Surveillance Marketplace

Yung Au

November 2021

Surveillance as a Service

The European AI-Assisted Mass Surveillance Marketplace

Yung Au

NOVEMBER 2021

Oxford Commission on
AI & Good Governance

Contents

EXECUTIVE SUMMARY

This report examines the European marketplace that produces and exports AI-assisted surveillance systems to governments around the world. In particular, it looks at what we call "Surveillance as a Service" (SaaS): services and software that are provided for surveillance, and which consist of complex systems that are offered with user-friendly interfaces as well as continual maintenance, updates, and troubleshooting support (rather than a one-off purchase).

This analysis focuses on three examples of such services that have become particularly controversial of late: facial recognition and analysis; speech recognition and analysis; and behavioural analysis and nudging systems.

Estimating the market size of these industries is extremely difficult because of how varied the technologies themselves are. In addition, surveillance systems have long supply chains and a great number of components to make them operational, some more difficult to track than others. Along with the lack of transparency, estimating the number of manufacturers, intermediaries, buyers, and total revenue of sales presents significant challenges. Nevertheless, estimates from 2020 have pinpointed that the broader global facial recognition and analysis marketplace is worth around 3.86 billion USD, the speech recognition and analysis industry is worth 10–11 billion USD, and behavioural analytics is worth 401–891 million USD—with all these valuations projected to grow exponentially in the coming decade.

This examination of Europe's contribution to the surveillance market is based on evidence from civil society groups and journalists, materials from companies and public agencies, secondary sources, expert commentaries, public documentations on litigation, and pre-existing data sets. Sorting through this body of evidence, this report examines the kinds of services that are being offered, the various use cases, and the controversies that have been engendered. In the case of all three types of service, there appear to be urgent concerns around the technologies themselves, the business practices surrounding them, and how these systems are deployed. This report also notes considerations beyond the cases discussed here—including how much of today's surveillance operations lies beyond artificial intelligence and machine learning systems or SaaS, the immense research and development industry of future surveillance technologies, and the many data pipelines that feed into these systems.

This report reinforces what many civil society groups, journalists, and independent researchers have urged before. As the overlap between AI technologies and mass surveillance applications continues to grow, so does the potential for harm. Whether this comes through testing surveillance technologies on unsuspecting populations, using data without user consent, or exporting surveillance technologies that may be misused by governments, the unfettered development of SaaS systems threatens human rights. Based on the latest evidence about the development of Europe's SaaS market, wider policy and regulatory interventions are urgently needed. This includes the need to:

1. Implement more stringent regulatory mechanisms for Europe's surveillance industry, including sales moratoriums and bans of certain technologies that produce the most harm.

2. Implement more rigorous evaluation and regulation over the far-reaching effects of the surveillance industry beyond the EU.

3. Enact proportionate and clear sanctions for breaching rules and guidelines.

4. Better empower oversight mechanisms on the design, development, and deployment of machine learning applications in ways that do not place the burden of reporting human rights violation on civil society groups, journalists, researchers, and individual citizens.

Many uncertainties remain about the future of surveillance and the industries which make these operations possible. While the landscape continues to resist any easy definitions, it is clear that if left under-regulated, this marketplace has widespread potential for lasting harms and consequences.

1 INTRODUCTION

Today's surveillance marketplace is vast. This is, in part, due to the vast scope of what "surveillance" can entail, the myriad actors involved, and the growing intersection with artificial intelligence (AI) and machine learning (ML) systems. While there may be reasons to monitor populations, our troubled histories of technology and surveillance, and the complicated ways in which surveillance is becoming increasingly entangled with AI, have prompted concern about this global marketplace. This is exacerbated by recent controversies about overreach and harm caused by government surveillance around the world.

To better understand the convoluted supply chains of AI-assisted mass surveillance, this report examines one particular part of the chain—the European marketplace. Being home to numerous surveillance companies, start-ups, and research projects, European countries are among the most prolific exporters of a wide array of surveillance technologies, ranging from computer vision technologies to commercial malware. In mapping and tracing some of these flows, this report asks a number of questions: What is the state of the European surveillance marketplace that sells AI-assisted mass surveillance technologies through Surveillance as a Service (SaaS) to governments around the world? There is currently a lot of hype surrounding artificial intelligence and machine learning, so how exactly do today's surveillance technologies intersect with AI systems? Who sells what types of surveillance systems, and to whom? What are the implications of this growing marketplace for the future?

This report will focus on three broad types of AI-assisted SaaS that have become especially controversial of late: facial recognition and analysis systems; speech recognition and analysis systems; and behavioural analysis and nudging systems (see Table 1).

Definitions and Scope

Professor David Lyon defines surveillance as the "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction".[1,p.14] In this conceptualisation, surveillance functions as a process of social sorting—where people and behaviours are categorised, evaluated, and shaped in some way. Professor Simone Browne further argues that surveillance, both past and present, reifies socially constructed categories such as race in order to segment and tame populations.[2] The range of activities that could potentially be counted as surveillance is immense, including, for instance, projects to sequence a population's genetic information, gaze-tracking systems that seek to optimise behaviour, observations done through CCTV, and analysis of credit history records.

Similarly, the datafication of humans and their behaviour is a central component of artificial intelligence and machine learning systems which rely on data troves to train algorithms to recognise patterns and make predictions. In today's smart systems, the collection of extremely detailed and fine-grain information alongside hyper-personalisation appears to be the default.[3] Here, intentional efforts are needed to resist this standard (see, for instance, DuckDuckGo's search engine, which does not personalise search results based on browsing history and is outside of the norm of such technologies). It is thus unsurprising that the overlap between surveillance technology and artificial intelligence and machine learning technologies is growing at an unprecedented pace.

To narrow the scope of this large intersection, this report looks at the overlap of artificial intelligence and machine learning and surveillance in those marketplaces that sell Surveillance as a Service to governments in service of mass surveillance projects.

Table 1. Types of AI-assisted SaaS

Type	Examples of research streams	Examples of companies that incorporate these services
1. Facial recognition and analysis	Machine vision, facial expression/emotion psychology	IDEMIA (formerly Morpho, SAGEM, and SNECMA) and Noldus
2. Speech recognition and analysis	Machine listening, voice psychology	Nexa Technologies (formerly Amesys) and FinFisher conglomerate (Gamma Group, FinFisher, Trovicor, Elaman)
3. Behavioural analysis and nudging	Draws from broad fields including nudge theory, persuasion science, and behavioural psychology	Cambridge Analytica, Behavioural Insights Team

What counts as "AI" has long been debated.[4] This report makes use of the current definition in the draft EU AI Act as a starting point: "'Artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." The current list of techniques and approaches in Annex I is as follows:

- Machine learning approaches, including supervised, unsupervised, and reinforcement learning, using a wide variety of methods including deep learning
- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, and expert systems
- Statistical approaches, Bayesian estimation, search, and optimisation methods

The focus here is on when AI systems are core to surveillance technologies. For instance, a chat-box assistant that is supported by an AI system made for the purpose of answering queries about a point-and-a-click camera would not be included here because the camera would still function without the AI-assisted chatbot.

This report specifically examines Surveillance as a Service (SaaS). The advent of the Internet has seen the rise of Anything as a Service or (X)aaS (X as a Service), which are services that provide endpoints for customers to interface with (usually with cloud computing and API-driven components). Some examples include Artificial Intelligence and/or Machine Learning as a Service (outsourcing the experimentation and use of AI systems without large initial investments), Back End as a Service (outsourcing the behind-the-scenes elements of an application and its maintenance so customers can focus on the front end), and Big Data as a Service (outsourcing elements of storing, cleaning, and analysing large amounts of data). All of these follow a pattern whereby complex and expensive systems are simplified into "plug and play" services that are maintained over time. Here, the client does not necessarily need to have technical knowledge of the systems at hand.

SaaS is thus defined here as services and software that are provided for surveillance, and which consist of complex systems that are offered with user-friendly interfaces as well as continual maintenance, updates, and troubleshooting support (rather than a one-off purchase).

Finally, this report concentrates on technologies that may assist mass surveillance (the indiscriminate surveillance of an indefinite or large number of people) which are being sold to government agencies.

2 METHODOLOGY

This report surveys secondary sources and pre-existing data sets to compile a partial overview of the SaaS marketplace. This includes media reports, reports from non-governmental organisations (NGOs), government reporting on the sale and distribution of surveillance technologies, and companies' self-reporting of their own technology and client use cases.

It draws on long-running, intensive efforts to shed light on public–private partnerships for surveillance, including in-depth investigative pieces, curated databases, crowdsourced projects, and data leaks including:

- Privacy International's archive of evidence, reports, and litigation on the surveillance industry, such as Big Brother Incorporated[5] and the Global Surveillance Industry,[6] which maps over 528 companies that supply surveillance technologies
- The Citizen Lab's series of in-depth reports into surveillance technologies, including technical dissections and audits of surveillance software[7]
- Access Now's series of investigations and campaigns on biometric surveillance and digital identification projects[8]
- Amnesty's series of investigations and campaigns on mass surveillance[9]
- Article 19's investigations and campaigns on biometric technologies and human rights[10]
- Electronic Frontier Foundation's Atlas of Surveillance, a US-centric data set of police technology[11]
- Reports from European Digital Rights on privacy and data protection[12]
- Carnegie Endowment for International Peace's 2019 report, *The Global Expansion of AI Surveillance*, which catalogues over 75 countries that use smart city technologies, facial recognition, and smart policing for surveillance[13]
- WikiLeaks's Spy Files, an archive of leaked documents relating to various surveillance companies[14]

- Steven Feldstein's Commercial Spyware Global Inventory, which presents an inventory of commercial spyware procured by governments[15]
- Other news reports from Biometric Updates, LexisNexis, Google Scholar, and Google Patents

Using these sources, this report explores specific cases as defined above. The data presented here is not exhaustive nor necessarily representative. Instead, the aim here is to examine some of the surveillance flows emerging from Europe, summarise patterns, and examine the implications of this growing marketplace.

The sources here are subject to some common limitations in the field. This includes the reliance on open-source data, with many of the above reports and data sets often overlapping, using the same sources for their data. There is also a particular bias towards English-language sources and investigations, as well as efforts that tend to focus geographically on Europe and the US. Nevertheless, these explorations provide invaluable insights into the elusive political economy of mass surveillance systems.

3 THREE EXAMPLES OF SURVEILLANCE AS A SERVICE

This section examines three types of Surveillance as a Service that have become particularly controversial of late: facial recognition and analysis; speech recognition and analysis; and behavioural analysis and nudging. The report lays out these three clusters of SaaS based on the general streams of AI systems they rely on—computer vision, machine listening, and behavioural data analytics respectively. These categories are not exclusive and overlap in many ways (for instance, facial recognition can be paired with voice recognition for multimodal biometric identification). Nevertheless, this section aims to parse out exactly the involvement of AI in each case.

Facial Recognition and Analysis

Facial recognition has come to the fore as one of the most notable and controversial practices of AI-assisted mass surveillance by governments. The intersection of AI and facial recognition is relatively straightforward, with facial recognition being a significant subsection of computer vision research—a stream of AI research that focuses on training computers to derive meaningful information from visual inputs. Beyond facial recognition, various other surveillance technologies involve computer vision systems. For example, object recognition systems have been used for surveillance practices such to detect the presence of a gun in an image, or for deploying automated licence plate readers. Action recognition has been used in an attempt to identify cases of shoplifting or loitering through the detection of action sequences. Signal processing technology has also been deployed in this arena—Headlight AI, for example, is a UK-based start-up that uses signal processing technology and 3D mapping to sense and map harsh environments for autonomous drones and robots.

Facial recognition and other computer vision technologies often fit into surveillance traditions of visually tracking populations, identifying "persons of interests", and profiling particular people. Facial recognition technologies have widespread applications beyond this and beyond government surveillance as well, and this broader market has an estimated value of around 3.86 billion USD in 2020.[16]

As of 2020, 109 countries are using or have approved the use of facial recognition/analysis for government surveillance.[17] These technologies are usually used as part of biometric surveillance (inferring identities), affect recognition (inferring emotional states and other information), and lie detection systems. Despite their widespread usage by governments, these technologies have been heavily criticised due to issues ranging from the bias embedded in these systems[18,19] and the lack of consent at various stages of a product's lifecycle,[20] to the flawed scientific basis of some of these models[20,21] and critiques about the business practices of surveillance companies.[22]

Some examples of European companies operating in this marketplace include IDEMIA (formerly Morpho), a French company that specialises in facial recognition technologies and that has served governments in Bangladesh, Burkina Faso, Costa Rica, China, France, Germany, Kenya, Iceland, Italy, Mali, Norway, Singapore, and the US. They have offered "plug and play" solutions for facial recognition for over a decade (see Figure 1 for an example).[23] These systems include MorphoFace, which offers a "biometric solution for face capture and matching in one single connected device",[24] and VisionPass, which offers a tool that provides "1-second verification through multiple angles and in all light conditions, and is resistant to all kinds of spoofing attempts".[25] Throughout IDEMIA's history, they have been implicated in various controversies, including alleged corruption in Bangladesh, Kenya, and the US. IDEMIA's facial recognition algorithms have also been shown to exhibit racial

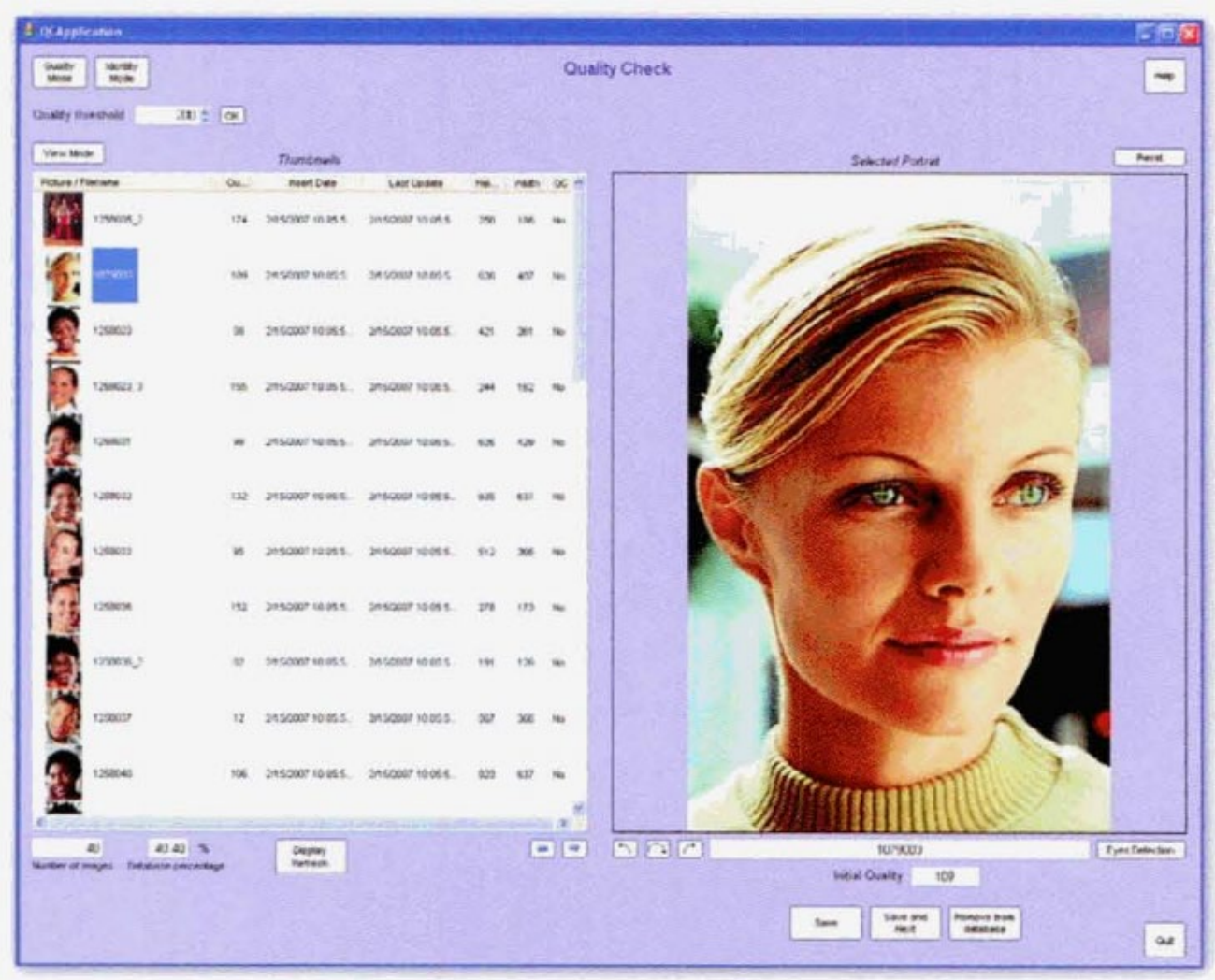


Figure 1. Screenshot from Morpho's report on their Face Investigate Pilot (2011), an earlier technology which sought to provide a user friendly face recognition system and was part of a series of feasibility studies on facial recognition (taken in September 2021, accessible here: https://www.wikileaks.org/spyfiles/document/safran/SAFRAN-2011-AnIntrto-en/SAFRAN-2011-AnIntrto-en.pdf) [23]

and gender bias.[26,27] More broadly, the company's government contracts have also been questioned by civil rights organisations, particularly concerning the vulnerabilities that arise when private corporations are given access to sensitive biometric data.[28]

Similarly, Noldus is a Dutch company that has sold facial analysis technologies (Figure 2)[29] to governments and public institutions in the US and China. Noldus maintains that their technologies are not for surveillance purposes and are designed for the study of human behaviour within government and research institutes. They assert that their focus is on extraction of micro-expressions and other facial inferences for behavioural research rather than identification.[30] For instance, their FaceReader technologies provide automated "recognition of a number of specific properties in facial images, including the six basic or universal expressions: happy, sad, angry, surprised, scared, and disgusted".[29]

Steps involved in Noldus's FaceReader technology include

1. "Face finding", where a "deep learning face-finding algorithm is used to locate a face in an image".
2. "Face modelling", where modelling techniques using deep neural networks are used to estimate the collection of landmarks in a given face and a compressed vector representation is produced about the face.
3. "Face classification", where classification of the facial expression takes place, including facial expression classification, valence calculation (whether the emotional state of the subject is "positive" or "negative"), arousal calculation (whether the test participant is "active"), action

unit classification (analysis of muscle groups in the face which are responsible for facial recognition), and subject characteristic analysis.

Separate models are available for FaceReader, such as modules for "East Asian people" and "babies between 6–24 months of age",[29] with the implication that Caucasian adults are the default. Furthermore, Noldus makes available add-on modules that can be used, for example, to analyse expressions from a group of participants (e.g., segmented by gender). The remote photoplethysmography module is another service, which aims to detect blood volume change in the tissue under the skin and infer things such as average heart rates (used for activities like lie detection).

These technologies assert that a wide variety of inferences are possible from a face. However, this premise has also been heavily critiqued. Researchers Vidushi Marda and Shazeda Ahmed argue that the development, sale, and deployment of emotion recognition technologies are inconsistent with human rights, with current systems relying on discredited scientific foundations, particularly "that facial expressions are universal, that emotional states can be unearthed from them, and that such inferences are reliable enough to be used to make decisions".[20,p.6] In an interrogation of the scientific foundations underpinning emotional recognition technologies, Luke Stark and Jesse Hoey argue that the concepts of affect and emotion are still intensely debated across disciplines and involve evaluative, physiological, phenomenological, expressive, behavioural, and mental components.[21] This complex array of processes that exist with many cultural differences are already difficult to pin down and the technical constraints in emotional recognition systems mean that these multi-dimensional and highly divergent processes are further reduced to biophysical signals such as facial expression, heart rates, and other proxies of emotion that fall short of the realities of human emotions. Furthermore, like facial identification algorithms, emotional recognition systems also exhibit discriminatory bias such as rating the faces of Black people as angrier and more contemptuous than white people.[31]

Speech Recognition and Analysis

Speech recognition, like facial recognition, has a relatively straightforward overlap with artificial intelligence and machine learning, and constitutes an important subdivision in computer audition/machine listening research—a stream of AI research that focuses on training computers to derive meaningful information from audio content. Other machine listening surveillance technologies currently in the market include gunfire locator algorithms which combine acoustic,

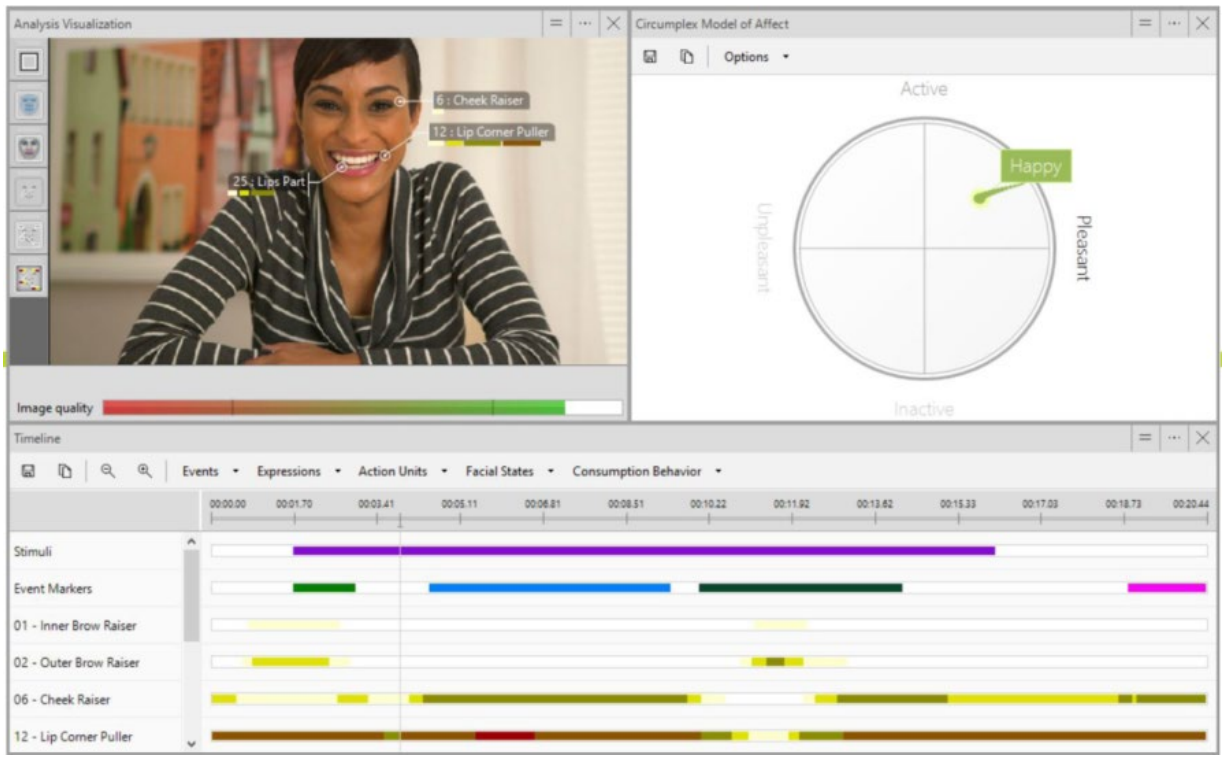


Figure 2. Screenshot from Noldus's FaceReader White Paper (2021); this module in particular offers the purported capability of distinguishing a genuine smile from a fake one (taken in September 2021, accessible here: https://www.noldus.com/resources/pdf/noldus-white-paper-facs.pdf) [29]

seismological, and optical detection techniques to detect gunfire incidences. Speech recognition technologies have many applications outside of government where this market is valued between 10–11 billion USD in 2020.[32,33] Governments often use speech recognition and analysis technologies in the context of speech biometrics and content analysis of audio data derived from lawful interception (legal access to private communications). Lawful interception has been a particularly controversial topic due to the extensive and covert nature of many of these operations—this is especially true of the invasive use of deep packet inspection (DPI) technologies and commercial malware to obtain communication at scale.

DPI technologies allow the examination of data being sent over computer networks. Like the other technologies, it has widespread applications beyond surveillance: common network traffic management toolkits use DPI technologies. The DPI market was estimated to be worth between 3 and 9 billion USD in 2020.[34,35] Commercial malware (also known as Malware as a Service) is the lease of software and hardware for carrying out lawful interception missions; for instance, using malware to infect personal devices in order to listen in on private conversations. As of 2021, at least 74 governments have bought spyware technologies, and the largest companies that supply this are headquartered in Europe and the US.[36,37] The commercial spyware industry has an estimated value of 12 billion USD.[36,37]

Most SaaS packages that offer such legal interception services tend to bundle DPI and/or commercial malware services along with speech recognition and analysis technologies. This is because the large quantities of audio data intercepted by authorities in the form of Internet communication, phone communications, and offline conversations in operations of mass surveillance often benefit from AI-assisted sorting. This can be seen, for example, in the case of Nexa Technologies.

Nexa Technologies (formerly Amesys) is a French company that is currently facing litigation for selling surveillance technologies to governments in the Middle East and North Africa region between the late 2000s and the early 2010s. These complaints were filed by the International Federation for Human Rights and the French League for Human Rights, who argued that the technologies sold by Nexa Technologies contributed to human rights violations of citizens in the region. The specific software they sold in the late 2000s was the Eagle system (Figure 3)[38]; following a name change, they continued to sell a similar but updated system called Cerebro. Both systems offer DPI technologies for intercepting communications, with additional support in terms of setting up monitor centres, training staff, and troubleshooting. These systems are offered with user-friendly interfaces for

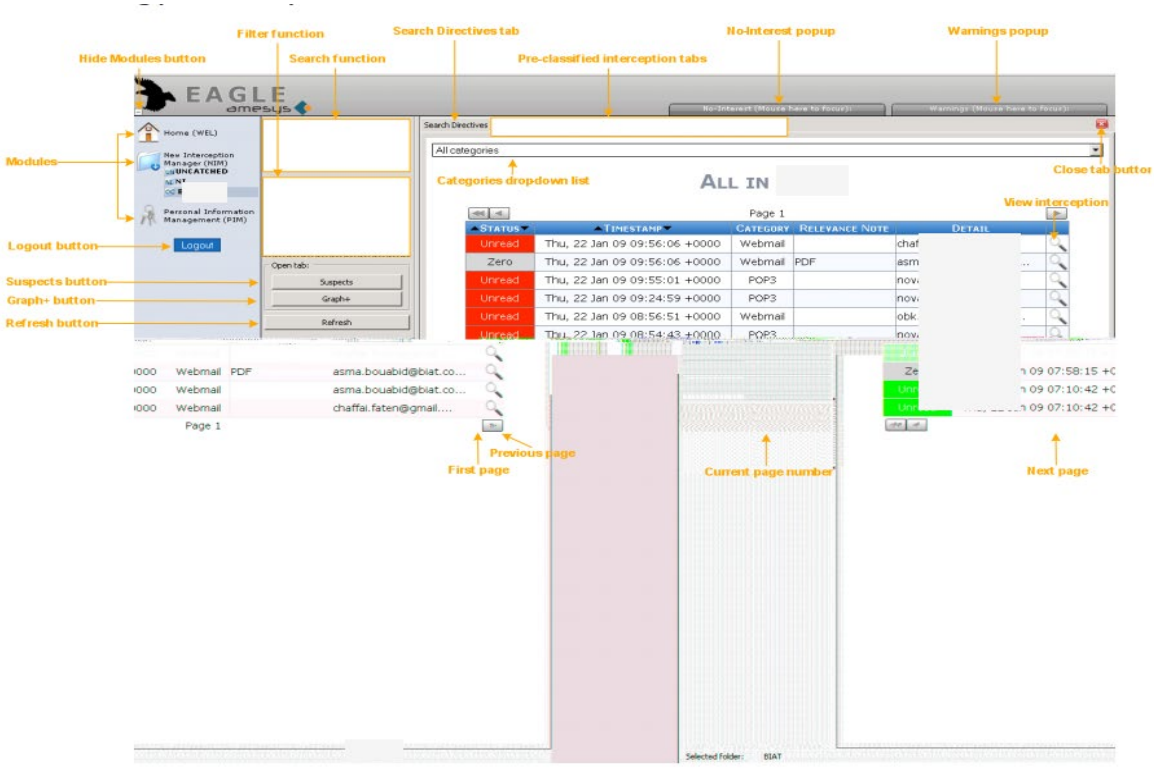


Figure 3. Screenshot from Amesys' Eagle Operator Manual which showcases its interface (taken in September 2021, accessible here: https://wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf) [38]

collecting, searching, and analysing intercepted data.

Many of the functionalities of their DPI technologies do not necessarily need AI. For example, they have rule-based sorting of data that relies on the manual updating of these rules for packet filtering. Other functionalities which would not necessarily require AI include basic search functions such as database queries or plotting network graphs and geo-location data. The intersection with AI and/or ML is more direct in what Nexa Technologies refers to as smart modules. In their previous system, the Eagle system, smart modules helped classify, categorise, sort, and search the large troves of intercepted communication. This included more complicated search and pattern recognition functions (topical and semantic analysis), automated traffic classification and analysis, and automatic voice transcription, translation, and speaker identification. The promotional materials for the Eagle system assert that

> facing the increasing number of voice communications at the scale of a nation, human operators are not any more capable of analysing these data. The automatic transcription can be combined with a module of speaker recognition. You will define a bunch of suspected people of whose voice is known. Afterwards, the system will automatically recognise them amongst all the others. This can also be used as an alarm trigger.[38]

The company is still in operation, however four Nexa Technologies executives were indicted in June 2021 for their roles in human rights violations through the export of their software and related services.[39]

Within the marketplace for commercial spyware, the use of spyware products known as FinFisher or FinSpy is particularly widespread. This spyware suite allows its operators to infect computer and phone devices in order to gain access to stored data and to gain control over integrated cameras and microphones. FinFisher/FinSpy has been supplied to at least 34 governments around the world for capturing communications in projects of lawful interception. These technologies are developed and distributed by a combination of companies consisting of Gamma Group (UK and Germany), FinFisher (Germany), Trovicor (Germany), and Elaman (Germany). The combined services of these companies include the selling and maintenance of spyware, DPI, data analytics, and voice biometric technologies as well as services to setup monitoring centres.

The companies involved in FinFisher have faced numerous legal challenges and official complaints.[40] For instance, Gamma Group is currently facing a lawsuit brought against it in 2018 by four activists in the UK. The company is accused of selling spyware to governments, despite knowing that their technologies would be used to crack down on human rights activists and to suppress dissidents. In this case, the company is accused of not only providing the spyware suite, but also the training needed and continual technical support throughout the crackdown on activists. The executive directors of FinFisher and Elaman are also facing criminal charges brought against them in 2019 for selling spyware to the Turkish government without an export licence.

Speech recognition technologies are also shifting beyond just sorting through the content of auditory inputs. Other developments such as voice categorisation and computational psychiatry seek to make inferences from speech patterns about personality traits, emotions, mental health status, and demographic categories.[41] These, like in the case of emotion recognition technologies, have been controversial. For instance, Access Now in particular has called for a ban on the automated recognition of gender and sexual orientation through speech recognition on the basis that these technologies are premised on scientifically flawed foundations and put LGBTQ+ lives at risk.[42] Likewise, Dr. Beth Semel argues that the idea that we can objectively and accurately infer complex human attributes, such as mental illness, from vocal data lacks an empirical basis, and that even the most benign voice analytic technologies run the risk of reproducing scientific racism and other modes of domination.[43]

Behavioural Analysis and Nudging

Behavioural recognition is the large-scale analysis of behavioural and demographic data for surveillance and behavioural shaping. This is the broadest category of the three types of SaaS discussed here, as almost any data analytics, market research, public relations, lobbying, consulting, and profiling can potentially fit here. Nevertheless, this capacious category of activities has become a mainstay of mass surveillance around the world. This category of surveillance involves monitoring populations and influencing behaviours at scale. Examples include policy implementation to encourage crime deterrence, good citizenship behaviour (such as timely tax payments), and environmentally friendly behaviour.

This type of surveillance is often assisted by AI systems to

conduct large-scale analysis and is also known as "nudging", "persuasion science", "micro-targeting", "profiling", "predictive policing", "data mining and data science", and "behavioural psychology". This landscape has many grey areas and is close to "dark-patterned AI systems", "social engineering", and "subliminal techniques". The last of these is explicitly discussed in the draft EU AI Act:

> The prohibitions covers [sic] practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour *in a manner that is likely to cause them or another person psychological or physical harm*. [italics added]

The line between the more accepted forms of behavioural analysis and nudging appears to be whether the behavioural shaping is operationalised for "social good" or "social bad", and certain actors retain the power of arbitrating this.

As indicated above, there is a notable crossover between behavioural recognition technologies and facial and speech recognition in cases where behavioural information is extracted (instead of or in addition to identification functions). Like the other technologies discussed here, behavioural analytics has widespread applications beyond government, and the broader market for "User and Entity Behaviour Analytics" was estimated at 401–891 million USD in the year 2020.[44–46]

Within this large category of SaaS, micro-targeting has become particularly notorious since it came to public attention during the Cambridge Analytica scandal. Cambridge Analytica (a subsidiary of SCL) was a UK political consulting company that was involved in over 200 elections around the world, as well as with various military departments in the UK and the US.[47,48] Cambridge Analytica provided a variety of services geared towards shaping public opinion on political and other issues, including large-scale data scraping and collection, monitoring and analysis, cloud computing, and help in creating operation centres (Figure 4)[49].

In 2018, information about Cambridge Analytica's misuse of up to 87 million Facebook profiles in order to micro-target users with political advertisements was disclosed by news outlets such as the New York Times, the Guardian/Observer, and Channel 4 News, with intel from whistleblowers Christopher Wylie and Brittany Kaiser as well as from researchers such as Dr. Emma Briant. In response to the media reports, public outrage, and campaigning efforts, the UK's Information Commissioner's Office pursued investigations into the company. The US Federal Trade Commission also filed complaints against Cambridge Analytica and eventually negotiated settlements with its CEO Alexander Nix in 2019.

Cambridge Analytica officially closed its business in 2018, but former employees have regrouped in various ways, including through newly formed firms such as Data Propria, Emerdata, and more than 18 other companies, branches, and affiliates.[50] For instance, in 2018, a handful of former Cambridge Analytica staff launched Auspex International, a firm specialising in political influence in Africa and the Middle East. Like Cambridge Analytica, they specialise in several areas: behavioural and psychographic research; data science including using "AI and data science methods to make sense of patterns in the data" such as identifying latent motivations and emerging topics to "ultimately model, segment and target an entire population", and targeted communications and persuasive messaging on topics, policies, and media channels. In this venture, the company sets out to make clear certain principles including that "we only work for legitimate governments, political candidates and organisations … [and] focus efforts on positive change".[51] However, the company remains the ultimate arbiter of which governments are legitimate, and what comprises "positive change".

Another variety of behavioural recognition is nudging, and an important player in this field is the Behavioural Insights Team (BIT, also known as the "Nudge Unit"), which emerged from a branch of the UK government. BIT expanded into a private company in 2014, and seeks to apply "behavioural insights to inform policy and improve public services, following nudge theory".[52] They are owned by the employees themselves, the UK Cabinet Office, and Nesta, and have served government departments in Australia, Canada, France, Singapore, the UK, and the US. Some use cases they present on their website include trials on messaging to encourage offenders released on bail to turn up in court and messaging to encourage intervention as a bystander.

Ultimately, the category of behaviour analysis technologies is difficult to parse and catalogue as SaaS because companies can supply many different parts of the behavioural analysis pipeline (from data extraction to the implementation of insights to influence behaviour). For example, Chorus Intelligence is a UK-based company that specialises in data-cleaning software that is used by over half of the UK's police

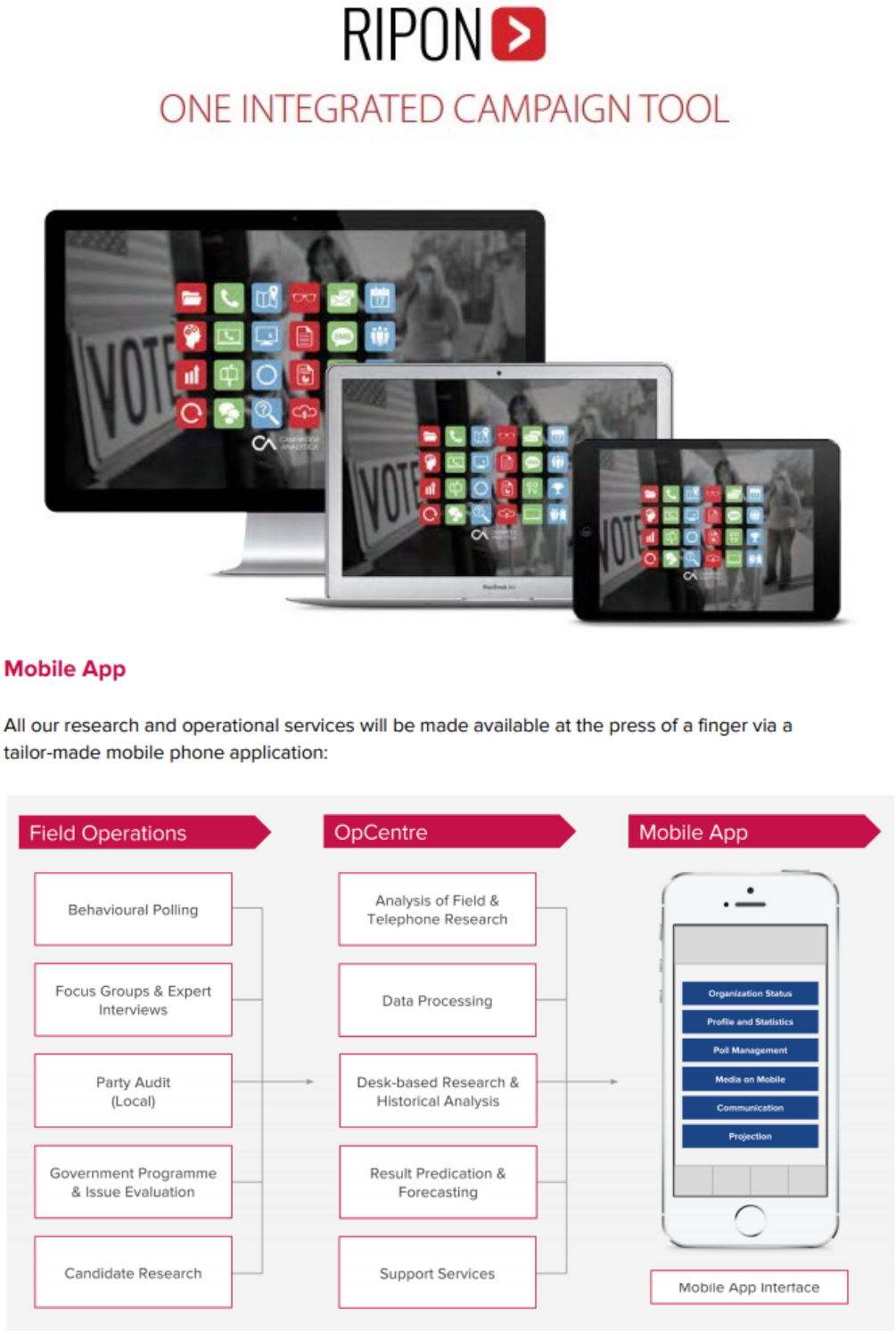


Figure 4. Screenshot from Brittany Kaiser's document leaks on Cambridge Analytica. This was part of Cambridge Analytica's promotional material detailing their integrated services (taken in September 2021, accessible here: https://ia803204.us.archive.org/35/items/ca-docs-with-redactions-sept-23-2020-4pm/FINAL%20Cambridge%20Analytica%20Select%202016%20Campaign%20Related%20Documents%20w%20Redactions_.pdf) [49]

forces, but their focus is very much on data wrangling and making raw data usable. Similarly, Clue is a UK-based company that sells software for investigation management used by over 18 police forces in Britain that aids at the stage of information gathering and collating. FUTR, another company based in the UK, creates chatbots with natural

language processing software to analyse the tone, emotion, and sentiment of messages, with the intention of sorting through low-risk calls made to emergency services in the UK. As more of our policing, government, and day-to-day administration becomes digitised, stored, and analysed, what can be counted as surveillance infrastructure becomes yet broader.

Other Considerations

The preceding was a brief overview into some of the categories of SaaS in the European marketplace. A wide array of other activities that would meet the initial criteria for SaaS have not been explored here due to their scope. First, for example, there are other specialised biometric technologies such as fingerprinting, smell recognition, DNA sequencing, electroencephalography, gait recognition, and gaze tracking. Second, there are systems related to electronic signals intelligence (ELINT). Third, there are specific technologies that support large-scale data systems such as census data, credit scores, criminal records, and health databases. Fourth, and most recently, there are technologies related to the many COVID-19 surveillance programs, such as contact-tracing systems and temperature-tracking systems.

Moreover, many vital aspects of mass surveillance also lie outside of the criteria that were set out. To begin with, there are important elements of surveillance beyond AI/ML systems. Professor Simone Browne in particular has traced the long and extensive history of surveillance which pre-dates the invention of any computer or digitisation processes.[2] There are important offline elements of surveillance, including the people conducting surveillance, profiling, and acting on this information. Much computerised surveillance similarly does not necessarily use AI/ML systems at its core.

Then there is AI-assisted surveillance that lies outside of SaaS. Internet service providers and social media companies and platforms often contribute to mass surveillance even if they do not sell SaaS. For example, surveillance can be conducted through legally binding data access requests where intermediary companies often have considerable latitude in how they respond to government requests for information.[53] There are also particular partnerships between law enforcement and technology companies, allowing traditional routes of data access to be circumvented. For instance, between 2018 and 2021, Amazon Ring brokered over 1,800 partnerships with US law enforcement agencies, which allowed for video recordings from users to be requested without a warrant.[54] Moreover, there are data brokerages that feed into the complex surveillance supply chain. For instance, the companies Babel Street (US) and X-Mode (US) have been found to supply location data extracted from a variety of apps to clients including US military contractors.[55] Finally, technology companies can also provide raw data that are core to surveillance systems, even if indirectly. For instance, the facial recognition firm Clearview AI scrapes images off Facebook and YouTube to train its models. Cambridge Analytica's method of gaining access to data through third-party actors is also increasingly becoming common practice.

A further aspect of mass surveillance that must be taken into account is the speculative surveillance industry, which feeds into SaaS. Much research and development (R&D) of surveillance systems is funded and undertaken in Europe. This is particularly notable as there are blurred lines for when a piece of surveillance technology is out of the R&D stage and ready for deployment. Here, European governments and funders have significant influence on what eventually emerges in the marketplace. For instance, one particularly contentious project is iBorderCtrl, which aimed to develop technology to identify and analyse micro-expressions on an individual's face in order to assess whether or not they were lying; in other words, an AI-powered lie detector. The endeavour has been critiqued for many reasons, including its faulty scientific foundations, but also because it was funded under the European Commission's Horizon 2020 programme.[56,57]

A final example of mass surveillance not considered here consists of the data sets and data pipelines that feed into SaaS. The data pipelines that feed into AI systems also importantly shape them.[58] For instance, Exposing.AI have produced detailed investigations into the WILDTRACK multi-camera person data set emerging from the École Polytechnique Fédérale de Lausanne and ETH Zurich. This data set has subsequently been used for further research and development on UAV aerial surveillance or person detection in the UK and China, as well as retail surveillance or pedestrian detection in the US and Spain. Likewise, the Oxford Town Centre data set from the University of Oxford has been used in over 60 research projects, from ones conducted by Disney and Huawei to those of research institutes in Japan, India, Israel, Singapore, Russia, the US, and elsewhere.[59]

The chart on the following page summarizes selected incidents in Europe's surveillance as a service industry.

SELECTED INCIDENTS IN EUROPE'S SURVEILLANCE AS A SERVICE INDUSTRY

Key: Business Operations | Investigative Reports (reports by NGOs, journalists, researchers and whistle-blowers) | Legal Claim | Legal Decisions

IDEMIA

- **Est 1842** — IDEMIA is formed by a combination of companies including Morpho, Défense Sécurité, Safran Group, Société d'Applications Générales d' Électricité et de Mécanique (SAGEM), and Imprimerie Oberthur. The oldest of these being the latter, founded in France, 1842.
- **2015-2017** — Legal claim made against Safran/Morpho by whistle-blowers accusing the company of fraudulent practices and for concealing how their fingerprinting software, which was used by the FBI, contains code created by a Russian firm. Legal claim and appeal dismissed two years later.
- **2017** — Oberthur Technologies (OT) and Safran Identity & Security (Morpho) merged to create OT-Morpho.
- The World Bank sanctions and debars OT for 2.5 years for bribery and corruption relating to a national ID project in Bangladesh. OT admits wrongdoing and reaches settlement agreement with World Bank.
- OT-Morpho renamed IDEMIA.
- **2017-2020** — The World Bank and the African Development Bank sanctions IDEMIA in Nigeria for fraudulent practices and corruption charges in relation to contracting processes.
- **2018** — IDEMIA placed on Burma Campaign UK's boycott list for working with the Burmese military on digital development projects.
- **2019** — Kenyan National Assembly votes for a 10-year ban on IDEMIA for allegedly interfering with the 2017 Kenyan elections. IDEMIA successfully appeals the ban.
- Gemalto Cogent, a US competitor, filed lawsuit alleging state officials illegally awarded contract to IDEMIA without a bid.
- **2020** — AET Europe, a Dutch competitor, files a lawsuit against IDEMIA Netherlands and the Dutch Ministry for Internal Affairs for unfair procurement processes. The lawsuit is dismissed later that year.
- Amnesty releases report implicating IDEMIA for selling surveillance technologies to oppressive regimes.

NEXA TECHNOLOGIES

- **Est 1979** — Bull was established in 1931, France, and it created a subsidiary named Amesys in 1979. Amesys was eventually sold and renamed as Nexa Technologies. They specialise in security solutions and products.
- **2011** — *Wall Street Journal* breaks news of Amesys supplying technology to an oppressive government to monitor citizens and suppress opponents.
- The International Federation for Human Rights (FIDH) and the League for Human Rights (LDH) file a criminal complaint at the Paris High Court against Amesys, alleging that they were complicit in human rights violation through their provision of surveillance technologies and services.
- **2012** — Electronic Frontier Foundation (EFF) releases report condemning Amesys for selling to authoritarian governments.
- The Paris High Court dismisses FIDH and LDH request to open a criminal investigation, arguing that there was insufficient evidence.
- Nexa Technologies was founded.
- **2013** — Reporters Without Borders named Amesys as one of five "Corporate Enemies of the Internet" and "Digital Era Mercenaries" for selling products that have been used to violate human rights.
- Bull sells Amesys to Nexa Technologies.
- **2017** — The French media outlet, *Télérama*, publishes report revealing Amesys/Nexa Technologies continue to supply updated surveillance system to oppressive regimes.
- FIDH and LDH file a second criminal complaint to the Paris High Court against Amesys, this time with further evidence they are complicit in human rights violation. A judicial investigation into the allegations is opened in December 2017.
- **2021** — Four executives of Nexa Technologies are indicted for complicity in torture.

GAMMA GROUP

- **Est 1990** — Gamma Group was founded in UK, 1990, where Gamma International (GI) is a subsidiary of. They specialise in selling surveillance technology and training for governments.
- **2012-** — Privacy International begins to investigate GI and the spyware suite it distributes, Finfisher - including submitting evidence to HM Revenue and Customs (HMRC); filing for judicial review of HMRC processes; and filing a criminal complaint to National Cyber Crime Unit about unlawful surveillance made possible by the spyware.
- EFF releases report warning about GI's business practices and for selling to authoritarian governments.
- CitizenLab releases its first report on the FinFisher Spyware Suite.
- **2013** — Reporters Without Borders named GI as one of five "Corporate Enemies of the Internet" and "Digital Era Mercenaries" for selling products used by governments to violate human rights.
- Five organisations file a formal complaint with the Organisation for Economic Co-operation and Development's (OECD) local reporting body, the National Contact Point (NCP), in UK and Germany against GI and Trovicor for alleged human rights violation by supplying surveillance equipment used against activists. German NCP dismiss investigation request.
- **2014** — The UK NCP accepts complaint against GI, determining they were in violation of OECD guidelines. In light of this, a series of steps are recommended for the company.
- Privacy International (PI) and the European Center for Constitutional and Human Rights (ECCHR) file a criminal complaint against GI in Germany. German court dismisses PI and ECCHR complaints later that year.
- "Phineas Fisher" hacks GI, releasing 40GB of data including client lists and source codes to the public. This prompts further analysis from organisations such as Privacy International, Netzpolitik, and Vice.
- **2018-** — Four claimants whose computers were targeted with the FinSpy program sue Gamma Group in the UK Courts for selling surveillance software which they allege was used to target human rights activists.

FINFISHER

- **Est 2008** — FinFisher, the company that developed the FinFisher/FinSpy spyware, was founded in Germany in 2008.
- **2012** — CitizenLab released its first report on the FinFisher Spyware Suite.
- NGOs, journalists and researchers continue reporting on the invasive spyware developed by FinFisher, including from Amnesty International, Article 19, Association For Progressive Communications, Citizen Lab, Digital Rights Foundation, EFF, Index On Censorship, Global Voices Advocacy, and Privacy International.
- Privacy International begins to investigate FinFisher and the spyware suite it created - including submitting evidence to HMRC, filing for judicial review of HMRC processes, and filing a criminal complaint to National Cyber Crime Unit about unlawful surveillance made possible by the spyware.
- **2019** — Four NGOs, The Society for Civil Rights (GFF), Reporters Without Borders Germany (RSF Germany), netzpolitik.org and The European Center for Constitutional and Human Rights (ECCHR) file a criminal complaint in Germany against several CEOs of FinFisher and Elaman for exporting surveillance software without an export license.
- **2020** — German authorities raid FinFisher's headquarters in Munich and its other premises during the investigations following the complaint filed by the four NGOs.

CAMBRIDGE ANALYTICA

- **Est 2013** — The Strategic Communication Laboratories Group (SCL) was founded in the UK in the 1990s, in which Cambridge Analytica (CA), a data analytic and consulting firm, was a subsidiary of.
- **2018** — *The New York Times* and *The Guardian/Observer* releases an exposé on how CA illicitly harvested data from millions of Facebook profiles, including with intel from whistle-blowers, Christopher Wylie and later on, Brittany Kaiser. Additional investigations by Channel 4 and researchers such as Dr Emma Briant further reveal inner workings of SCL's illicit operations.
- Following investigations and public outrage, US' Federal Trade Commission (FTC) opens investigation on Facebook and CA.
- UK and US lawyers launch a joint class action lawsuit against CA, SCL, & Facebook for the misuse of personal data.
- SCL and CA announces that they will cease all business operations. CA files for bankruptcy in USA.
- In April 2018, several former SCL staff form Emic Consulting, a data analytic firm.
- In May 2018, several former CA staff launch Data Propria, a data analytic firm.
- In July 2018, several former CA staff launch Auspex International, a data analytic firm.
- India's Central Bureau of Investigation begins an investigation into CA's data breach scandal.
- **2019** — FTC files settlement with CA's former CEO, Alexander Nix; administrative orders on future business conducts; to delete personal data collected from Facebook.
- The FTC sues CA for acts of deception and misuse of data.
- A UK court fines an SCL subsidiary £15,000 for failure to comply with information disclosures.
- Reports on how Emerdata, a company founded in 2017 by the former directors of CA, acquires most of SCL's companies prior to bankruptcies and appear to be continuing their operations.

NOTES & DISCLAIMERS – There are some inherent difficulties when mapping companies and their various winding timelines. This includes how firstly, there is a notable "Ship of Theseus" type of problem with many long-running companies. For instance, IDEMIA as it exists today is an amalgamation of companies that extend back to 1842 (Imprimerie Oberthur) through various mergers, acquisitions, and changes that occurred over the decades. Does the company that exists today also represent the various companies that were absorbed – including these company's histories of innovations, clientele, and controversies? Secondly, there is also the complication of size; some companies are truly large, larger than some countries, and this makes it hard to gather information and avoid acts of scape-goating when something does go wrong. Thirdly, we are also not implying causality in the order of events displayed here. We are simply laying out the difficult terrain pertaining to businesses in this industry. For instance, it appears to be common for companies to file legal claims against each other during tender processes. However, various things are worth noting. One being how important efforts from NGOs, journalists, and researchers are in unearthing and drawing public attention to when human rights violations are present – from the discovery stages to actual litigation and bringing corporations to court.

4 CONCLUSIONS

As the overlap between AI and mass surveillance continues to grow, the breadth of potential harm has risen in tandem. The European Commission recently released the draft EU AI Act in response to the urgent need for better regulation of emerging technologies. The proposed act in its current form covers certain instances of SaaS discussed above. For instance, it prohibits real-time remote biometric identification systems from being used in public spaces. However, it also includes a wide range of exceptions for law enforcement purposes, which detrimentally constricts what is prohibited to an extremely narrow range and moreover further legitimises the exceptions where usage of these technologies is allowed and justified.[60] Furthermore, if more careful regulation on the testing, development, and deployment of SaaS within EU territories is enacted without commensurate regulations in other countries or in EU export regulations, mixed global standards would be created. This could create situations whereby the EU might ban certain surveillance technologies from being used within EU territories but effectively encourage that same technology to be exported and tested outside of EU borders. A range of additional measures are crucially needed, otherwise we risk exacerbating the problems identified in this study of Europe's SaaS industry.

Human rights organisations have been urging the EU to halt the export of surveillance technologies from Europe to potentially oppressive regimes for over a decade.[5,61–64] However, despite the implementation of stricter export controls in Europe since the Arab Spring in 2011, when many European technologies were revealed to have assisted in the crackdown on protests, many of today's surveillance technologies used by oppressive governments are still made in the EU.[65] For instance, the current export regulation framework of the EU, the Dual-Use Regulation, still omits many instances of digital surveillance technologies, and processes to expand this framework remain heavily bureaucratised and slow-paced.[66,67] Furthermore, the problems in this area are not limited to exports by certain governments—all regimes can and do misuse surveillance technologies.

The causes for concerns are multiplied when many innovations of mass surveillance rely on uncertain scientific bases and where AI systems inherently rely on an iterative process—here, certain parts of the world are essentially sanctioned as laboratories for the newest technologies. Ultimately these models require trials in real-world conditions, somewhere, somehow. This is an ongoing pattern in the broader tech landscape, with the Global South being treated as a testing ground for software and technologies prohibited in the West.[68,69] Likewise, this is another area where ethics shirking, the practice of reaching for much lower standards of ethics in certain localities, becomes commonplace.[70] As seen here, many surveillance companies and technologies are associated with controversies, lawsuits, and real-life harm. All too frequently, these only come to light after extensive efforts from civil society, journalists, and researchers—and often only when it affects the West. Likewise, only certain actors are empowered to litigate against companies in Europe when something does go wrong.

The SaaS marketplace is growing rapidly, and developing in a way which makes it more entangled with AI technologies, so that it is increasingly complicated to categorise it and keep it in check. Many controversial transactions around AI-assisted mass surveillance technologies still occur under the radar, with corporate entities often difficult to pin down in this complex supply chain—especially when such actors go through countless name changes, mergers, and splintering. How then, should we navigate this increasingly complex and precarious landscape?

5 RECOMMENDATIONS

Given the state of the surveillance landscape, it is clear we need more stringent governance processes. Recommendations will always vary depending on the context and locality. However, as a start:

1. Implement more stringent regulatory mechanisms for Europe's surveillance industry, including sales moratoriums and bans of certain technologies that produce the most harm.

   There are a host of groups that have demonstrated the need for the imposition of a moratorium on various aspects of the surveillance marketplace—with some suggestions being stopgap measures until better governance processes are in place, and others being more permanent bans. One such example is the Reclaim Your Face coalition, a group of civil society actors within the EU who have called for a wider ban on biometric mass surveillance practices including its development.[71] Another proposal is that urged in a joint open letter by 174 organisations and experts which calls on states to

implement an immediate moratorium on the sale, transfer, and use of surveillance technology in light of the NSO spyware disclosures in the summer of 2021.[72] AI Now has likewise called for a moratorium on all uses of facial recognition in sensitive social and political domains—including policing, education, and employment—where facial recognition poses risks that cannot be remedied retroactively.[73] Researchers Vidushi Marda and Shazeda Ahmed have also asserted that the design, development, and deployment of emotional recognition be banned given the racist foundations of these systems and the incompatibility of it with human rights.[20] The Citizen Lab and the former United Nations Special Rapporteur on Freedom of Opinion and Expression, David Kaye, as well as Edward Snowden, have urged bans and regulations on the trade of spyware,[74] while Carly Kind from the Ada Lovelace Institute has recommended a voluntary moratorium on facial recognition from companies themselves.[75]

2. Implement more rigorous evaluation and regulation over the far-reaching effects of the surveillance industry beyond the EU.

   Stringency here will require an examination of the far-reaching effects of regulation, including an evaluation of the double standards and displacement effects of regulations that will likely be far-reaching, such as the EU AI Act. For instance, if high-risk AI systems are banned in the EU but exports are still allowed and investment in them will continue, will this merely facilitate the deployment and testing of high-risk AI systems in other countries? Ethics shirking practices must be more systematically evaluated and regulated. As seen here, the EU is a particularly important exporter of SaaS, and so the implications of its regulation or non-regulation will have long-lasting impacts beyond this region.

3. Enact proportionate and clear sanctions for breaching rules and guidelines.

   Technology companies often manage to evade or wriggle out of proportionate sanctions—for instance, when fines are just the "cost of doing business". Likewise, sanctions often occur only after harm has been done and only if it garners enough public outrage. This can be seen perhaps most clearly in the high-profile case of Cambridge Analytica, where a great many investigative and litigation resources were needed for this controversy to come to light—and even then mainly only around its operations in the US and the UK.[47] And while Cambridge Analytica itself has declared bankruptcy since the controversy became public, observers have argued that the actual fines incurred as a result of this controversy were negligible, and that its operation appears to live on in other entities.[76,77]

4. Better empower oversight mechanisms on the design, development, and deployment of machine learning applications in ways that do not place the burden of reporting human rights violation on civil society groups, journalists, researchers, and individual citizens.

   There should be more systematic reporting, audits, and scrutiny of potential human rights violations. Despite the current regulations in place in the EU, including the Dual-Use Regulation, export licensing processes, and Organisation for Economic Co-operation and Development (OECD) guidelines, much of the investigative work on surveillance abuse is carried on by civil society groups and journalists and researchers who are often restricted by resources and data access. With no signs of the industry slowing down, there needs to be better mechanisms in place to ensure we are not just addressing controversies and harm after the fact.

There remain many uncertainties about the future of surveillance and the industries which make these operations possible. While the landscape continues to resist any easy definitions, it is clear that, left under-regulated, this marketplace has widespread potential for harm and lasting consequences.

6 REFERENCES

1. Lyon, D. Surveillance Studies: An Overview. *Canadian Journal of Sociology* **33**, 471–475 (2008).

2. Browne, S. *Dark Matters: On the Surveillance of Blackness*. (Duke University Press, 2015).
3. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. (Profile Books, 2019).
4. Au, Y. A New AI Lexicon: An Electric Brain. *A New AI Lexicon* https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-an-electric-brain-77a81f3ce446 (29 June 2021).
5. Privacy International. Big Brother Incorporated. *Privacy International* http://www.privacyinternational.org/report/658/big-brother-incorporated (9 November 1995).
6. Privacy International. *The Global Surveillance Industry*. (Privacy International, 2016).
7. Citizen Lab. Citizen Lab Targeted Threats Archives. https://citizenlab.ca/category/research/targeted-threats/ (n.d.).
8. Access Now. Access Now Campaign Archive. *Access Now* https://www.accessnow.org/campaign/ (n.d.).
9. Amnesty. Amnesty Mass Surveillance Archive. https://www.amnesty.org.uk/issues/mass-surveillance (n.d.).
10. ARTICLE 19. When Bodies Become Data: Biometric Technologies and Free Expression. *ARTICLE 19* https://www.article19.org/biometric-technologies-privacy-data-free-expression/.
11. Electronic Frontier Foundation. Atlas of Surveillance. https://atlasofsurveillance.org/ (2020).
12. EDRI Privacy and Data Protection Archive. *European Digital Rights (EDRi)* https://edri.org/our-work?pillar=privacy-and-data-protection.
13. Feldstein, S. The Global Expansion of AI Surveillance. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (2019).
14. WikiLeaks. WikiLeaks - The Spy Files. https://wikileaks.org/the-spyfiles.html (2014).
15. Feldstein, S. Commercial Spyware Global Inventory. **2**, (2020) doi:10.17632/csvhpkt8tm.2.
16. Grand View Research. Facial Recognition Market Size & Trends Report, 2021-2028. https://www.grandviewresearch.com/industry-analysis/facial-recognition-market (2021).
17. Surfshark. Facial Recognition Map. *Surfshark* https://surfshark.com/facial-recognition-map (2020).
18. Buolamwini, J. & Gebru, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In *Conference on Fairness, Accountability and Transparency* 77–91 (PMLR, 2018).
19. Benjamin, R. *Race After Technology: Abolitionist Tools for the New Jim Code*. (Polity, 2019).
20. Marda, V. & Ahmed, S. *Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights*. (Article 19, 2021).
21. Stark, L. & Hoey, J. The Ethics of Emotion in Artificial Intelligence Systems. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* 782–793 (Association for Computing Machinery, 2021). doi:10.1145/3442188.3445939.
22. Privacy International. Facial Recognition Technologies (FRT). https://privacyinternational.org/learn/facial-recognition (2021).
23. Safran Morpho. An Introduction to Morpho Face Investigate Pilot. https://www.wikileaks.org/spyfiles/document/safran/SAFRAN-2011-AnIntrto-en/ (2011). Accessed September 2021.
24. IDEMIA. MorphoFACE: The New Facial Recognition Solution from Safran Identity & Security. *IDEMIA* https://www.idemia.com/press-release/morphoface-new-facial-recognition-solution-safran-identity-security-2017-03-14.
25. IDEMIA. VisionPass: Facial Recognition Access Control. *IDEMIA* https://www.idemia.com/facial-recognition-access-control (14 October 2020).
26. Harwell, D. Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use. *Washington Post* (19 December 2019).
27. Simonite, T. The Best Algorithms Still Struggle to Recognize Black Faces. *Wired* (22 July 2019).
28. ACLU. Major Face Surveillance Company Releases Dystopian Tracking Tool. *ACLU Massachusetts* https://www.aclum.org/en/publications/major-face-surveillance-company-releases-dystopian-tracking-tool

(24 June 2019).

29. Noldus. Noldus FaceReader White Paper. https://www.noldus.com/resources/pdf/noldus-white-paper-facs.pdf (2020).
30. Noldus. Noldus Press Release Response to Amnesty. http://docs.dpaq.de/16825-noldus.pdf (2020).
31. Rhue, L. *Racial Influence on Automated Perceptions of Emotions*. (Social Science Research Network, 2018). doi:10.2139/ssrn.3281765.
32. IMARC. Voice and Speech Recognition Market Size, Trends and Forecast 2021-2026. https://www.imarcgroup.com/voice-speech-recognition-market (2021).
33. Mordor Intelligence. Voice Recognition Market (2021-26). https://www.mordorintelligence.com/industry-reports/voice-recognition-market (2021).
34. *Global Deep Packet Inspection (DPI) Industry Report by Global Industry Analysts*. (Global Industry Analysts, 2021).
35. *Deep Packet Inspection (DPI) Market Size Report by Verified Market Research*. (Verified Market Research, 2021).
36. Feldstein, S. Governments Are Using Spyware on Citizens. Can They Be Stopped? *Carnegie Endowment for International Peace* https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019 (21 July 2021).
37. Woodhams, S. & O'Donnell, C. The Global Spyware Market Index. https://www.top10vpn.com/research/global-spyware-market-index/ (12 May 2021).
38. Amesys. Amesys Eagle Operator Manual. https://wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf (2011). Accessed September 2021.
39. International Federation for Human Rights. Q/A Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted. *International Federation for Human Rights* https://www.fidh.org/en/region/north-africa-middle-east/egypt/q-a-surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa (2021).
40. The Citizen Lab. Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry. *The Citizen Lab* https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ (12 December 2018).
41. Leufer, D. Sonic Surveillance: Why You Don't Want AI Snooping on You. *Access Now* https://www.accessnow.org/ai-snooping/ (30 June 2021).
42. Access Now. Ban Automated Recognition of Gender and Sexual Orientation. https://act.accessnow.org/page/79916/action/1 (2021).
43. Semel, B. The Body Audible: From Vocal Biomarkers to a Phrenology of the Throat. *Somatosphere* http://somatosphere.net/2020/the-body-audible.html/ (21 September 2020).
44. The Business Wire. $4.6 Billion User and Entity Behavior Analytics Market - Global Trajectory & Analytics to 2027. *The Business Wire* https://www.businesswire.com/news/home/20210127005439/en/4.6-Billion-User-and-Entity-Behavior-Analytics-Market---Global-Trajectory-Analytics-to-2027--ResearchAndMarkets.com (27 January 2021).
45. GlobeNewswire. *Global User and Entity Behavior Analytics Market to Reach $4.2 Billion by 2026*. (GlobeNewswire, 2021).
46. Market Data Forecast. *Global User and Entity Behavior Analytics Market (2021 – 2026)*. (Market Data Forecast, 2020).
47. Ghoshal, D. Mapped: The Breathtaking Global Reach of Cambridge Analytica's Parent Company. *Quartz* https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/ (2018).
48. Briant, E. Cambridge Analytica Map. *Propaganda Machine* https://www.propagandamachine.tech/ca-map (2020).
49. Cambridge Analytica 2016 Campaign Related Documents (Part of Document Leaks from Brittany

Kaiser). https://archive.org/details/ca-docs-with-redactions-sept-23-2020-4pm (2020). Accessed September 2021.

50. Grothaus, M. Auspex International Is the New Cambridge Analytica. *Fast Company* https://www.fastcompany.com/90202005/auspex-international-is-the-new-cambridge-analytica (13 July 2018).
51. AUSPEX. What We Believe. *AUSPEX International* https://www.auspex.ai/what-we-believe (2021).
52. Behavioural Insights Team. Behavioural Insights Team - About Us. https://www.bi.team/about-us/ (2021).
53. Ebert, I. The Tech Company Dilemma. Ethical Managerial Practice in Dealing with Government Data Requests. *Zeitschrift Für Wirtschafts- Und Unternehmensethik* **20**, 264–275 (2019) doi:10.5771/1439-880X-2019-2-264.
54. Bridges, L. Amazon's Ring Is the Largest Civilian Surveillance Network the US Has Ever Seen. *The Guardian* http://www.theguardian.com/commentisfree/2021/may/18/amazon-ring-largest-civilian-surveillance-network-us (18 May 2021).
55. Cox, J. How the U.S. Military Buys Location Data from Ordinary Apps. *Vice* (16 November 2020).
56. Gallagher, R. & Jona, L. We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive. *The Intercept* https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/ (26 July 2019).
57. Sánchez-Monedero, J. & Dencik, L. The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of IBorderCtrl. *Information, Communication & Society* 1–18 (2020) doi:10.1080/1369118X.2020.1792530.
58. Crawford, K. *The Atlas of AI*. (Yale University Press, 2021).
59. Harvey, A. & LaPlace, J. WILDTRACK. *Exposing.Ai* https://exposing.ai/datasets/wildtrack/ (2021).
60. Veale, M. & Borgesius, F. Z. Demystifying the Draft EU Artificial Intelligence Act. *ArXiv* (2021) doi:10.9785/cri-2021-220402.
61. Amnesty International. Q&A: Coalition Against Unlawful Surveillance Exports (CAUSE). https://www.amnesty.org/en/latest/news/2014/04/questions-and-answers-coalition-against-unlawful-surveillance-exports-cause/ (4 April 2014).
62. FIDH. Surveillance Technologies 'Made in Europe': Regulation Needed to Prevent Human Rights Abuses. https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe-1-2.pdf (2014).
63. Maurer, T., Omanovic, E. & Wagner, B. *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*. 46 (New America, 2014).
64. Timm, T. Spy Tech Companies & Their Authoritarian Customers, Part I: FinFisher And Amesys. *Electronic Frontier Foundation* https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys (16 February 2012).
65. Franke, J.-D. A Year in Surveillance. *About:Intel* https://aboutintel.eu/a-year-in-surveillance/ (30 December 2020).
66. Amnesty International. EU Companies Selling Surveillance Tools to China's Human Rights Abusers. https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/ (21 September 2020).
67. IFEX. Monitored and Targeted: Sale of Surveillance Technology Puts Lives of MENA Activists at Risk. *IFEX* https://ifex.org/monitored-and-targeted-sale-of-surveillance-technology-puts-lives-of-mena-activists-at-risk/ (25 December 2020).
68. Amrute, S. & Murillo, L. F. R. Introduction: Computing in/from the South. *Catalyst: Feminism, Theory, Technoscience* **6**, (2020).
69. Arora, P. Decolonizing Privacy Studies. *Television & New Media* **20**, 366–378 (2019) doi:10.1177/1527476418806092.
70. Cowls, J., Png, M.-T. & Au, Y. *Some Tentative Foundations for "Global" Algorithmic Ethics*. (Social Science Research Network, 2019).
71. ReclaimYourFace: Ban Biometric Mass Surveillance. *Reclaim Your Face* https://reclaimyourface.eu/ (2021).
72. Joint Open Letter by Civil Society Organizations and

Independent Experts Calling on States to Implement an Immediate Moratorium on the Sale, Transfer and Use of Surveillance Technology. *Amnesty International* https://www.amnesty.org/en/documents/doc10/4516/2021/en/ (2021).

73. Crawford, K. *et al. AI Now 2019 Report*. (AI Now, 2019).
74. Anstis, S., Deibert, R., Kenyon, M. & Scott-Railton, J. *The Dangerous Effects of Unregulated Commercial Spyware*. (Citizen Lab, University of Toronto, 2019).
75. Kind, C. Letter: Companies Can Adopt a Voluntary Moratorium on Facial Recognition. *Financial Times* (24 January 2020).
76. Cadwalladr, C. Cambridge Analytica Has Gone. But What Has It Left in Its Wake? *The Observer* (6 May 2018).
77. Witt, J. & Pastenack, A. The Strange Afterlife of Cambridge Analytica and the Mysterious Fate of Its Data. *Fast Company* https://www.fastcompany.com/90381366/the-mysterious-afterlife-of-cambridge-analytica-and-its-trove-of-data (26 July 2019).

ACKNOWLEDGEMENTS

We are grateful to Dr. Tim Curnow, John Gilbert, Mark Healy, Dr. Lucy Hennings, Srujana Katta, Lisa-Maria Neudert, and Flora Seddon for their contributions to this report.

For supporting our Oxford Commission on AI & Good Governance we are grateful to the Adessium Foundation, Ford Foundation, Luminate Foundation and Open Society Foundations. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the Commission and do not necessarily reflect the views of the University of Oxford, our founders, or individual commissioners. Ethical oversight of research at the University of Oxford is done by its Central University Research Ethics Committee. This research was approved under the CUREC number SSH_OII_CIA_19_074.

ABOUT THE AUTHOR

Yung Au is a doctoral researcher at the Oxford Internet Institute and with Oxford University's Programme on Technology and Democracy (DEMTECH). Her work looks at surveillance technologies, the industries that underpin these infrastructures, and the future of this landscape. She is also a Clarendon and Global Rotary Scholar (Hong Kong Harbour and Princes Risborough), as well as a Global History of Capitalism Scholar (2021-22).

ABOUT THE OXFORD COMMISSION ON AI AND GOOD GOVERNANCE

The mission of the Oxford Commission on AI and Good Governance (OxCAIGG) is to investigate the artificial intelligence implementation challenges faced by governments around the world, identify best practices for evaluating and managing risks and benefits, and recommend strategies for taking full advantage of technical capacities while mitigating potential harms of AI-enabled public policy. Drawing from input from experts across a wide range of geographic regions and areas of expertise, including stakeholders from government, industry, and technical and civil society, OxCAIGG will bring forward applicable and relevant recommendations for the use of AI for good governance.

oxcaigg.oii.ox.ac.uk

Oxford Commission on AI & Good Governance. Written & researched by Yung Au (2021). *Surveillance as a Service*. Working paper 2021.4, Oxford, UK: Oxford Commission on AI & Good Governance. 22pp.

Retrieved from: https://oxcaigg.oii.ox.ac.uk