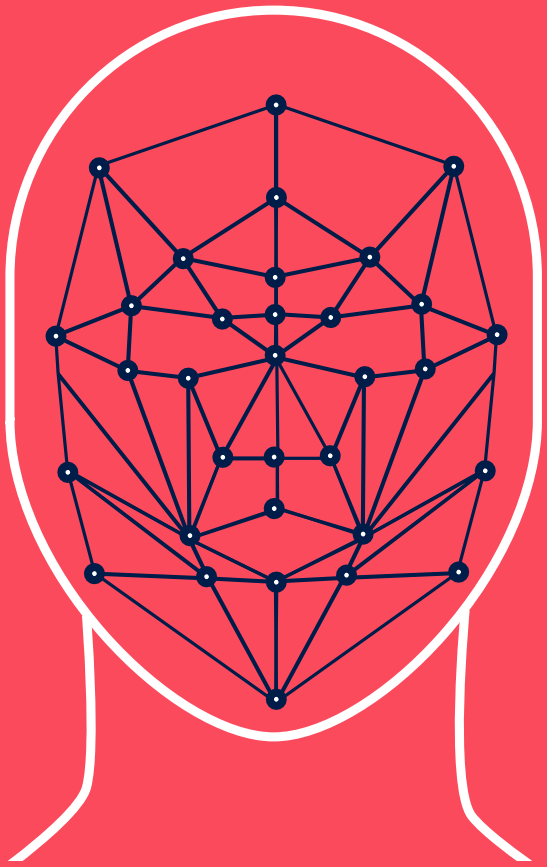
BEYOND THE FACE:
BIOMETRICS AND SOCIETY



Edited by
Ella Jakubowska, Andrej Petrovski & Danilo Krivokapić

ACKNOWLEDGEMENTS

We would like to thank our colleagues from the SHARE Foundation for all the support and contributions in the process of writing this book, as well as all the work they invested in fighting against biometric mass surveillance in Belgrade.

An immense thanks to all partner organisations from the ReclaimYourFace initiative.

Finally, we express absolute gratitude to every single person who contributed to the #hiljadekamera initiative, their generous support and appreciation was the main fuel for our work.

Thank you.

Credits:

Executive Editors

Andrej Petrovski & Danilo Krivokapić

Editor

Ella Jakubowska

Authors

Technology: Bojan Perkov

Legal: Jelena Adamović & Duje Kozomara

Practical: Mila Bajić & Duje Prkut

Proofreading

Una Dimitrijević & Milica Jovanović

Art direction and Design

Olivia Solis Villaverde

Arwork

“The architecture of a face recognition system”
by Vladan Joler

Publisher

SHARE Foundation

2023

CONTENTS

INTRODUCTION

In January 2019, the Serbian Minister of Internal Affairs made a groundbreaking announcement on national television, revealing their collaboration with Huawei, the Chinese tech giant. This partnership was poised to transform Belgrade into the first capital in Europe covered by thousands of cameras equipped with facial recognition capabilities. This announcement set off alarm bells for us, and we recognised the urgent need for immediate action, lest the streets of Belgrade undergo an irreversible transformation.

After nearly five years of relentless opposition to the introduction of face recognition surveillance in our city, involving three Ministers of Internal Affairs in Serbia, two withdrawn Draft Laws, numerous meetings, and countless hours devoted to research, campaigning, and advocacy, we made the decision to pen a book. Despite our familiarity with navigating uncharted waters, the realisation that the government was boasting about surveilling the entire population using AI technology presented us with a formidable challenge. Fortunately, we received support from individuals within our city and from partners facing similar threats worldwide, without whom our work would have been impossible.

This book is one of the most comprehensive explorations of how biometric systems are being used around the world and the laws (or lack of) which prescribe this. Whilst it does not profess to be exhaustive, it gives a snapshot of the global state of biometric surveillance in 2023. It is aimed at anyone wanting to better understand what biometric mass surveillance is, why we should care, and what can give us hope in the face of powerful state and private actors.

A standout theme throughout this book is the serious harm that these systems can lead to and the extreme violence which they facilitate. Traumatic wrongful arrests, eugenics, ethnic cleansing, exclusion, pushbacks and persecution are at the heart of biometric mass surveillance practices.

These practices in turn are driven by a global biometric surveillance industry where profits are privileged over people and our rights, and by states who believe – despite an abundance of evidence to the contrary – that these

systems contribute to a secure society. Each of the three sections of this book recognises that biometric technologies, and how they are used, are intrinsically a political issue.

Another key finding is just how difficult it is to uncover information about what's truly going on. From technical specifications, through to procurement processes and actual deployments: biometric systems have been shrouded in secrecy, further tipping the power balance between those who watch on the one hand, and those that get watched on the other.

There are likely to be many more abuses hidden in plain sight. The authors of this book have been reliant on, and are deeply grateful for, the work of journalists, lawyers, researchers and civil society groups who have fought tirelessly to expose the truth. On the regulatory front, dozens of data protection authorities, as well as independent supervisors like the Scottish Biometrics Commissioner and the NYPD Comptroller, are doing vital work to bring information to the public. However, these groups are all chronically under-resourced.

The legal situation across the world is changing rapidly, even in the final stages of writing this book. Delicately-brokered attempts to outlaw public facial recognition in some US states and in the EU have come under fire from politicians claiming that they will help fight serious crime. Moratoria are enacted then withdrawn, and efforts to regulate fizzle out. This is despite the fact that in the course of researching this book, we did not find even a single example of biometric mass surveillance technologies keeping people safe or contributing to justice – but a landslide of evidence of the harms.

KEY TERMS

Artificial intelligence (AI) — the ability to perceive, analyse and understand information by machines, which can be applied to autonomously perform tasks in different fields, such as speech recognition, computer vision or natural language processing.

Biometrics — an umbrella term to refer to the field, the measurement of features to turn them into biometric data, and/or the subsequent processing of biometric or biometrics-based data.

Biometric data — personally-identifying data relating to someone's face, body, or other physical or physiological characteristics (face, gait, etc.), usually that have been processed into a machine-readable format (template) with some connection to a person's identity. Some jurisdictions, such as the EU, state that the data must be able to "allow or confirm" a person's unique identity in order to be biometric (for example, a template of a person's face) and are only sensitive when used for the "purpose" of unique identification.

Biometric features — the physical and physiological features (face, eye, voice) before they have been processed to generate the biometric or biometrics-based data.

Biometric identification — the process of predicting the identity of a natural person by comparing their biometric data against a specific database or multiple databases (e.g. national ID database, database of wanted persons) above a certain threshold of probability.

Biometric mass surveillance (BMS) practices — the use of a system which captures and/or processes multiple people's biometric features at once, and which makes it possible that any of those persons might not be aware of it happening. As such, BMS practices are most commonly seen in public spaces, and are usually linked to systems that can identify people – although this is not necessary for the system to constitute BMS. This definition does not cover uses such as unlocking your personal phone, as long as they are genuinely consensual.

Biometric surveillance — a system which monitors people's biometric features in any way that is not under the full control and consent of the individual data subject.

Biometrics-based data — data that may not initially seem to personally identify someone (e.g. hair colour, skin colour, emotion) and have been processed into a machine-readable format. We note, however, that with the increase in video capture power, many of these data are or will soon be able to uniquely identify a person. Even without this ability, their processing can still be equally intrusive or harmful. As such, whilst this book uses the term "biometrics-based data" for clarity, we do not consider this to be a robust or scientific distinction. Instead, we advocate for biometrics-based data to be given the same (high) protections as biometric data.

Computer vision — an area of artificial intelligence which allows machines to analyse and understand information acquired from various visual inputs, such as digital images or video materials.

Eigenface — a visual representation of an eigenvector facial image as perceived by the human eye.

Eigenvector — in computer vision, a mathematical object which represents variability or deviation between the characteristics of a specific human face and an average value of all faces contained in a dataset.

Facial detection — a technical method of determining if a video or digital image material contains human faces, which is performed by automated means.

Facial recognition — a system/process to identify people based on their face biometrics. It can be used in real-time, often known as **live facial recognition (LFR)**, or after the fact, known as **retrospective facial recognition.**

Facial recognition technology (FRT) — as above, but usually refers to the whole system rather than the process.

Machine learning (ML) — the process of teaching machines to autonomously make predictions or decisions based on creating a mathematical model from data used for training.

Minoritised — following the Equinox RJI, we use the term "minoritised" for people or communities that have been constructed as non-dominant,

particularly those pushed to the margins of society (for example migrant communities and poor communities). In particular, we prefer this term to "vulnerable", thereby recognising that these communities are not vulnerable but have been put in precarious or vulnerable positions as a result of state policies and practices.

Moratorium — a temporary or time-limited ban on, or pause of, (in this context) certain biometric technologies. It may be limited to their use, or may also cover their development and deployment.

Neural networks — a method of artificial intelligence which teaches machines to process information so that they can find similarities or differences between data inputs in a supposedly similar way to the human brain.

People on the move — individuals or groups who are migrating for a number of reasons, including but not limited to seeking asylum. We privilege this term over others such as "migrants", which are often used with negative connotations, and which may also be used to suggest that only some categories of people on the move should be protected. However, we reassert that all persons on the move have rights and deserve protection.

Principal Component Analysis (PCA) — a statistical technique used to analyse large datasets and extract an average of key characteristics, i.e. the principal components of data.

Racialised — following the work of the Equinox Racial Justice Initiative (RJI), we use the term "racialised" to refer to people or communities who have been ascribed a perceived racial or ethnic identity, largely in the Global North. This includes Black and Brown communities, Muslim communities and Roma and Sinti people.

Remote Biometric Identification (RBI) — a term usually used in the EU context, as it is derived from the EU's AI Act. It refers to any identification done "at a distance", using biometric data.

Securitisation — specifically in the context of people on the move, "securitisation" can be seen as a purported security-focused approach to migration and border policies, within which people on the move are perceived as a risk to be managed and an external threat, rather than as human beings seeking assistance.

Training datasets — structured data (i.e. uniformly-prepared data for digital machine processing) which are fed to the system in order to train machines to perform specific functions. For example, in the case of computer vision systems, the training datasets consist of millions of different digital images either of human faces or various objects, depending on the type and intended purpose of the system.

Video surveillance system — a connected system for capturing video footage, often a closed-circuit television (CCTV) system.

TECHNOLOGY

INTRODUCTION

Starting with the basic technological processes that underpin biometric technologies, this section charts the development of increasingly sophisticated artificial intelligence systems. Over the last decade, these systems have transformed from performing relatively simple actions like spotting objects, into an exponentially complex landscape of processes for recognising, profiling, and making predictions and decisions on the basis of people's faces, bodies and behaviours.

The human mind has always been a key inspiration for research and development into computer vision. Yet an essential difference persists. Whilst the individuality of faces or the ridges and valleys of fingerprints make them ideal for algorithmic analysis, biometric recognition functions in an inherently reductionist way — where parts of our faces and bodies become machine-readable "objects".

In the late 1980s and into the 1990s, computer scientists and researchers grappled with how to convey human faces in machine-readable formats. The concepts of *eigenfaces* and *eigenvectors* allow us to understand that in order to "see" faces, facial recognition systems have to analyse how far any particular face is from a composite "average" face. At the same time, these coordinate systems represent the data with which they were fed and the decisions of those that fed them — in the case of these early systems, white men.

Those falling outside the machine's frame of reference for making sense of the world and determining what is "normal" are thus bound to be excluded and discriminated against. Such examples are deeply revelatory of how — as researchers such as Joy Buolamwini, Timnit Gebru and Deborah Raji have long emphasised — biometric technologies encode and reproduce human biases and discrimination. Algorithms are therefore a critical instrument of power for those that create them and set the rules by which they process data.

Through the process of Principal Component Analysis (PCA), we can further see how modern biometric processing is in fact based in crude stereotypes and even eugenic theories suggesting that a person's qualities

can be read in their face. Facial recognition systems developed in recent years by Google and Facebook have both labelled Black people as monkeys, emphasising just how deeply embedded these discriminatory ideas are in contemporary biometric systems.

These developments have all contributed to conditions whereby it is easier, faster and cheaper than ever before for states and corporations to roll out cameras and sensors, to store footage and reference images, and to apply facial recognition algorithms and other forms of analysis and profiling. Companies have used "the cloud" to make supercharging surveillance capabilities as easy as downloading an app on your phone; high-definition video has become a reality even in poor lighting conditions; and patents reveal developments that can recognise people even as their faces move and contort.

The increasing ease by which spaces that we all rely on to live our lives can be put under permanent surveillance has even become a key selling point for companies. We see how Huawei has marketed their "smart" technologies to landlords and small security operations — meaning that biometric mass surveillance is no longer the preserve of central governments. This decentralisation of biometric surveillance is matched by the technologies themselves, which increasingly promise the camera's inbuilt capabilities to spot intruders or shifts in crowd behaviour, eliminating the need for expensive operations rooms equipped with dozens of screens and blurring traditional boundaries between hardware and software.

In one particular example from Huawei, a system boasts capabilities including tagging (bookmarking parts of footage), creating automated blocklists for people behaving "abnormally", tracking people's trajectories (a feature also promoted by Amazon), and other tools that allow the creation of the world's most advanced panopticon. At the same time, many of these companies, Clearview AI and PimEyes included, warn their users that these tools should not be used in this way — a hypocritical statement given that mass surveillance is at the core of their design.

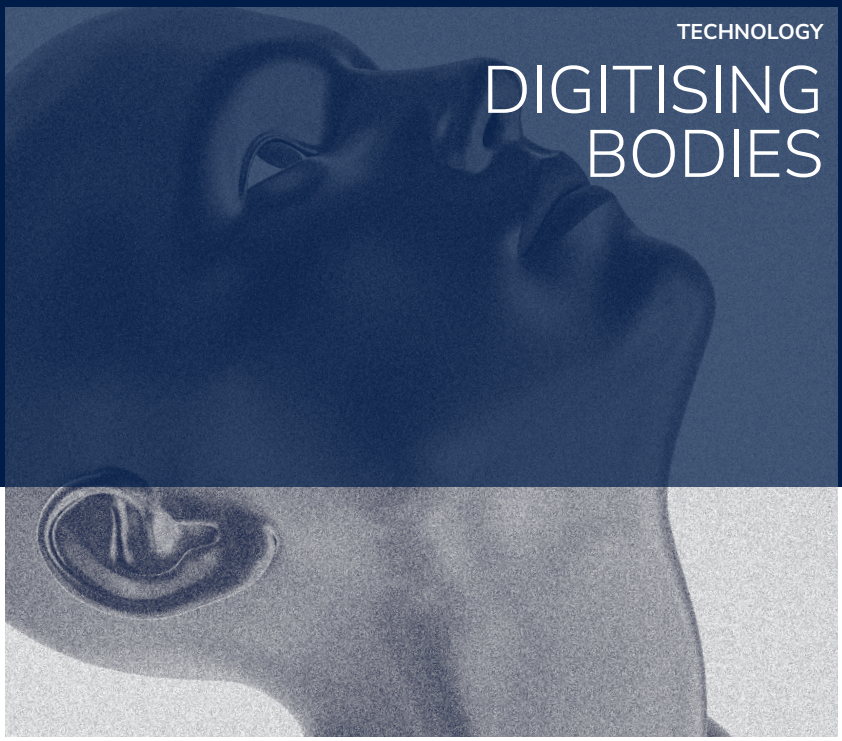
These systems also profile people's behaviours and perform other types of profiling — such as of people's emotions — in ways that question whether regulators to date have focused too much on identification use cases (where the goal is to find the name, reference, or other unique characteristic of a person or persons) and not enough on protections for use cases where

identification is not the goal (for example because the aim is to profile them based on their hair colour, regardless of who they are).

This section also hits on an essential problem, which is the extent to which companies have been able to set the agenda for how technologies can be used. IBM, for example, claimed to have stopped selling facial recognition to US police in the wake of the murder of George Floyd, but these claims have never been independently verified. And Microsoft's long-standing promise to retire emotion recognition technologies was, at the time of writing, still to be enacted.

The very fact that these companies have decided to enact moratoria on their own products and services hints at just how dangerous these systems are; at the same time, it also emphasises just how important it is not to allow them to make decisions that can have such far-reaching repercussions on our civil liberties.

Despite a seemingly technical and mathematical veneer, we can see that the development of these systems is and has always been deeply human. Racism and other forms of discrimination have masqueraded as technical objectivity. With patents and marketing materials opening a window into the biometric surveillance industry, it is clear that no millimetre of our faces or bodies is off-limits.



TECHNOLOGY

DIGITISING BODIES

COMPUTER VISION

BACKGROUND

To understand how machines observe, perceive, and make sense of objects and data — human faces in particular — we need to take a more detailed look at the logical framework of biometric data-processing systems. An illustrative system for this report will be one performing facial recognition, which remains the most prevalent and studied form of biometric recognition in surveillance contexts.

The concept of computer vision is of key importance for understanding the processing of images by machines. Machines or systems trained for computer vision can not only perceive and recognise objects or other visual representations in photos and videos, but are also trained to make sense of what they see. For example, they may process certain information from the

data and draw conclusions, depending on the purpose or needs for which the system is designed. Therefore, computer vision systems can be applied to numerous scenarios, from recognising whether an object, such as a car, is present in a surveilled area, to recognising a car with a specific licence plate number.

In order to explain what this means in practice, common examples of computer vision include the following:[1]

- Image classification: the system analyses what is presented in an image and marks it as belonging to a specific category or class, e.g. an animal, a person, or a vehicle;
- Object detection: the system detects whether a specific image category is present in a visual input, such as a video stream, e.g. detecting whether a person appears in a specific area;
- Object tracking: if an object from a defined category is detected in a visual input, the system can track and record its movements and positions across time and place;
- Content-based image retrieval: the system can search for and find images based on their content (e.g. colour).

One of the necessary preconditions for the development of a computer vision system, or any other system which can be trained to learn autonomously (known as "machine learning"), is for the system to be trained with a large amount of data. These data serve as an input value for learning, i.e. for the system to make sense of the data it receives and processes.

The quality of the system also needs to be tested and verified on other datasets before it is ready for use, to ensure that it can perform the required tasks to the expected level of accuracy. Machine-readable image datasets, which can contain hundreds of thousands, or even millions, of digital photographs of faces of an equally large number of different people, are used for the purpose of training facial recognition systems. The photos contained in the dataset can be faces of real people, which can create significant legal and ethical problems. Alternatively, the photoset can be synthesised, i.e. digitally generated by graphic processing.

Especially in the case of images of real people, these mass datasets have usually been collated in a broader social context which reflects historical

patterns of discrimination. This includes the decisions about who gets included in datasets, whether or not they have given their permission, as well as seemingly "technical" — but actually deeply subjective — decisions about how camera film and flashes work, which have led them to work best for white skin.[2] This causes machines such as those used in facial recognition to be trained on often fallible, non-representative and deeply problematic data.

As Vladan Joler and Matteo Pasquinelli explain, "dataset bias is [further] introduced through the preparation of training data by human operators".[3] This especially refers to the sensitive and painstaking process of data labelling. For image datasets, this means marking every image with tags describing it ("house", "tree", "door", "desk") which is easiest in the case of objects. However, when this is done on photos of people, any offensive, racist or otherwise discriminatory terms which are used to describe them will end up being reflected in the data, and therefore the trained system.[4]

For example, both Google and Facebook have rightfully come under fire for their computer vision systems mislabelling Black men as monkeys.[5] Google has publicly struggled to fix this problem, with their purported fix being to prevent the system from attributing the label "gorilla", rather than addressing the underlying bias and discrimination found in, and perpetuated by, the system.[6] This further emphasises just how difficult it is to resolve such issues, which seem to have become embedded in the fundamental designs of Google and Facebook's machine learning systems.

Perhaps the best known image dataset of real people (mostly public figures such as athletes, artists and politicians) is Labeled Faces in the Wild (LFW), created by researchers at the University of Massachusetts, which contains more than 13,000 photographs collected from the public internet. This dataset was made with the intention to study the problem of unconstrained facial recognition technology, as well as to provide the research community with more insights into face verification, which could help them advance their research. In the context of the dataset bias, the dataset disclaimer states that many groups, such as children, women, people older than 80, or of certain ethnicities, are not well represented.[7]

An example of a synthesised dataset is Digi-Face 1M, released in 2022, which contains more than one million photographs associated with around 110,000 identities. The authors claim that Digi-Face 1M tackles the common issues of models trained on photo datasets of real people, such as ethical issues,

labelling errors and data bias, since they created synthetic images from high-quality head scans which were obtained with consent from a small number of people.[8] However, even though the technical process of creating the dataset may not be as problematic compared to datasets with photos of real people, the biases of the people putting together these datasets can equally lead to discriminatory outcomes.

Also, it should be noted that systems which process biometric data will follow different steps depending on the desired function of the system. In particular, biometric verification and identification need to be distinguished. With verification, biometric data are used to confirm a person's identity based on their previously stored authenticators (1-to-1 comparison), usually in order to gain access to certain data or services. Examples of this are unlocking a mobile phone with a fingerprint or facial scan, or using a passport with a biometric chip to pass through an electronic passport control gate at airports. On the other hand, biometric identification is based on determining the identity of a person or persons by comparing their data against a database containing biometric data of numerous other individuals (1-to-many comparison). These databases can be relatively small (e.g. a list of wanted fugitives) or encompass almost entire populations as in a national ID database. Police using a facial recognition system to determine whether a person filmed by CCTV cameras in the street is on their watch list of crime suspects is an example of biometric identification.[9]

Before we go into more detail about the practical implications and implementations, it is necessary to explain two key mathematical and statistical concepts on which facial recognition by computer vision is based. These are Principal Component Analysis (PCA) and eigenvectors.

ROLE OF PRINCIPAL COMPONENT ANALYSIS (PCA)

The concept of calculating "averages", and the statistical treatment of human physical appearances, goes back to the times when it was deemed possible to determine personal character traits, e.g. who is a "criminal" and who is a "normal" person, based on distinctive physical features, such as the shape of the face. This can be linked to eugenics, a term coined by Francis Galton, a British statistician, demographer and ethnologist.[10]

In her book "Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face", Lila Lee-Morrison reflects on Galton's work. Galton

created "composite portraits" in the late 19th century by photographing numerous faces on a single photographic plate, measured against crosshairs aligned against the centre of the face. By using this technique, Galton made composite visual representations of people from different social groups, for example those who were involved in crime, had certain illnesses, or were of a certain ethnicity, in order to classify people into what he referred to as "types".[11] This crude method, both from a technical and scientific standpoint, was baseless and enforced discriminatory stereotypes that continue to cause harm, particularly towards minoritised populations.

Today, the large quantities of data required for a machine learning system to be able to perform its function need to be analysed in a way that is logically possible for a machine to perceive, process and understand. Digital images, depending on their quality and size, consist of pixels, which are the smallest element that can be shown on a digital display.[12] Modern high-definition images can contain millions of pixels, which — when multiplied by thousands of different image files in a dataset — represents a high volume of data to process. However, there is a method to reduce the complexity of the data, known as Principal Component Analysis (PCA).

PCA as a method essentially comes down to reducing the dataset to specific values in order to preserve as much information as possible, whilst simplifying the data to only the essential elements, so that it can be more easily analysed and interpreted. With digital images, as Lee-Morrison explains, "PCA treats each facial image as a point or a vector on a grid with a high-dimensional space allowing for high degrees of variation". The goal is to receive a mean value from the average of each pixel contained in the facial images. With this in mind, the characteristics (i.e. values) of the face that deviate from the mean are used to differentiate between the images and therefore the faces of different people.[13]

Researchers Lawrence Sirovich and Michael Kirby applied PCA to a set of 115 faces of undergraduate students at Brown University of whom they took photos, in order to demonstrate the feasibility of this procedure. Their research was published in 1987. The resulting "average face" portrayed a blurry representation of a young dark-haired Caucasian male, which was unsurprising given the homogeneity of the input data, and would be crucial in understanding how a machine trained on such data perceives the notion of the "human face".[14]

Sirovich, Kirby: Average face image from their 1987 paper

This experiment shows us the basis for the perception bias built into facial recognition systems. If the machine system is trained and tested to perceive a very specific type of facial form within its set of rules, known as its "coordinate system", it is bound to be error-prone and discriminatory towards faces of people with different skin tones or facial features. As facial recognition systems have frequently been trained on white male faces, those that fall outside the coordinates are most frequently minoritised people and those who are most discriminated against in a society. The false claim that technology is "infallible" and superior to humans often leads to it being portrayed as the solution to deeply-rooted social problems, such as crime and security challenges. This faulty assumption will be covered in more detail through case studies in the following sections of this publication.

An integral part of computer vision and its application to recognising faces relies on mathematical objects which also have a corresponding visualised state — eigenvectors and the resulting eigenfaces.

EIGENVECTORS AND EIGENFACE

When images of people's faces need to be presented in a way that a machine can understand, perceive and derive information from, eigenvectors are the key mathematical element that is used. Named as a combination of the German word *eigen* (meaning "own", "peculiar", "private") and vector as a mathematical expression, these objects represent components based on which a machine can differentiate between many different human faces.[15]

In order to create the eigenvectors, Principal Component Analysis (PCA) needs to be applied to the images in the training set. Lee-Morrison explains that the resulting eigenvectors represent the "greatest degree by which the facial images may vary" from the average. The eigenvector is a "virtual model of 'known' faces and serves as a reference point for the classification of unknown faces", as Lee-Morrison describes it.[16] Therefore, it is essential for a face recognition system to work and be trained to understand and recognise any number of different faces, from different positions or angles and external influences such as lighting.

Eigenvectors are abstract objects which enable machines to see and differentiate between faces (i.e. people), but in order to get a better understanding of how they appear to human beings, we need to refer to the eigenface. When humans look at an eigenvector, it appears as a blurry, nondescript face-shaped representation, and does not say much about a specific person — "the greater the variation of the eigenvector, the more blurred the eigenface appears".[17] Or, to put it simply: the further from the "average" face that a particular image appears to be, the more blurred its digital representation will be.

An example of a set of eigenfaces[18]

In the early 1990s, researchers from the Massachusetts Institute of Technology (MIT), Matthew Turk and Alex Pentland, worked on eigenfaces in order to explore this method and its applications for recognising faces. They explained how the process works: "Recognition is performed by projecting a new image into the subspace spanned by the eigenfaces ('face space') and then classifying the face by comparing its position in face space with the positions of known individuals."[19] In the context of contemporary facial recognition systems, Turk and Pentland also envisaged that their approach could enable the recognition of new faces through the use of neural networks.[20] It is interesting to note that they also had in mind efforts to perform recognition of gender and interpretation of facial expressions by using the eigenface analysis method.[21]

Although it is only a construct, the dehumanising appearance of the eigenface can show us that by erasing visible facial distinctions, the identity of human beings can be reduced to a mathematical procedure. Eigenface helps us understand the difference between human and computer vision and is essential to the recognition process. Similarly to Galton's composite portraits, when these processes are applied in a setting where technosolutionist and technodeterminist views often influence actors who have the authority to decide on matters of human rights, discriminatory practices are bound to be reproduced, particularly when it comes to people in a vulnerable social position (e.g. people on the move, prisoners).[22]

Advances in biometric identification technology are also fuelling the almost exponential development of machine learning algorithms, which feed on data and knowledge extraction in order to perform tasks such as PCA to create eigenvectors, as explained. To provide more context, we now delve into neural networks and their application in computer vision.

NEURAL NETWORKS

MACHINE LEARNING AND BIOMETRICS

The development of advanced computer vision systems is not only focused on training a machine to perform a specific task, but also on making it possible for machines to autonomously make predictions and decisions in certain situations. The role of machine learning in today's society is often presented as a mystic force that enables artificial intelligence to flourish and expand. The more realistic point of view, argued by Joler and Pasquinelli, is that it is just another knowledge instrument, like many others developed throughout the history of humanity. As they point out, "it is more reasonable to consider machine learning as an instrument of knowledge magnification that helps to perceive features, patterns, and correlations through vast spaces of data beyond human reach."[23]

Machine learning depends on huge quantities of data, as well as algorithms that are becoming more sophisticated as the research in this area progresses. Algorithms are essentially instructions that define processes that the system needs to perform in order to create an output (result) from the data it is provided with, i.e. the input. Algorithms are therefore a critical instrument of power for those that create them and set the rules by which they process data. In that sense, valuable proprietary algorithms (e.g. those used by Big Tech companies for their products such as social networking platforms or search engines) are protected as trade secrets, which makes oversight on how they work and whether they have adverse effects very difficult — as will be further explored in the final section on Practice.[24]

Biometrics can most commonly be described as "the measurement and analysis of unique physical or behavioural characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity."[25] With the enormous potential of biometrics for analysis, statistics, surveillance, identity verification and other significant areas of research and development, biometric data have unsurprisingly found their way into machine learning. As with many other inputs, human biological characteristics can, at least from a technical standpoint, be easily digitised and prepared as structured datasets for machine learning purposes. Faces have distinctive features, fingerprints consist of ridges and valleys, while the textures of irises and the patterns of blood vessels in retinas can all be used for identification.[26]

Using data with such high variability, yet still specific enough for the principal components of a dataset to be extracted, provides the opportunity for the system to learn by making sense of patterns. This forms the basis for the system to understand connections between data and to perform more advanced tasks autonomously.

For example, we can differentiate between machine learning classification and machine learning prediction. Classification is used to recognise a particular object, assign it a label and categorise it: "An input file (e.g. a headshot captured by a surveillance camera) is run through the model to determine whether it falls within its statistical distribution or not. If so, it is assigned the corresponding output label."[27] The aim of machine learning prediction, however, is to predict outcomes or behaviour based on only a portion of available data, i.e. "...a small sample of input data (a primer) is used to predict the missing part of the information following once again the statistical distribution of the model."[28]

These machine learning scenarios can be applied in a number of settings and social contexts, most notably for biometric surveillance or other forms of social control. However, to get a better understanding of how machine learning systems reach an output from data they are being fed, it is necessary to discuss neural networks and their design. Convolutional neural networks in particular are important for advanced computer vision systems.

THE DEVELOPMENT OF NEURAL NETWORKS

A machine learning process called deep learning is designed to enable machines to make connections between information through a layered structure of artificially-interconnected nodes (or neurons). This enables a wide range of neural network applications in many products and services we encounter every day, such as computer vision, speech recognition, natural language processing, or recommendation engines.[29]

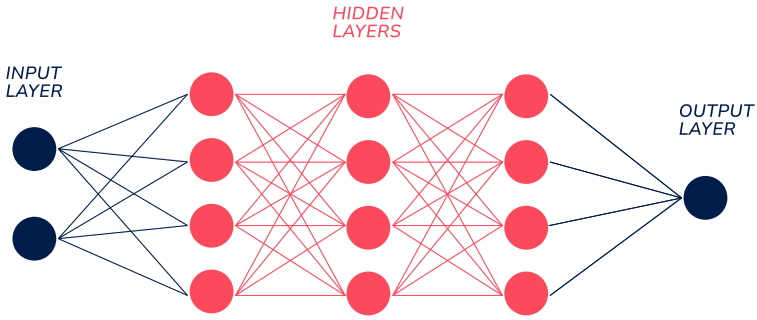
However, when neural networks are compared to human brain functions in a wider context, a study conducted at MIT has shown that caution is necessary before drawing comparisons. Namely, the analysis of more than 11,000 neural networks which were trained to simulate the function of the key component of the brain's navigation system, called grid cells, revealed they only produced such activity when given very specific constraints that are not found in biological systems.[30]

When it comes to the structure of a neural network, there are two general types of architecture:[31]

» **Simple neural network architecture**, starting with the input layer, where nodes process the data entering the system. The data then goes to the hidden layer, in which nodes analyse the data from the input layer or other hidden layers, as neural networks can have many of them. Finally, the output layer gives the final result based on the processed information in the entire network. The final (output) layer can have one or multiple nodes, depending on the complexity of the task. But if there is a binary result (yes/no, 1/0) expected, then the output layer will have just one node;

» **Deep neural network architecture**, which is structured in a more complex manner, consisting of numerous hidden layers with millions of interlinked nodes. The relations between the nodes are called "weights", which are values describing the influence of nodes on other nodes, i.e. whether they pass data on to further nodes or not. These networks typically require much larger quantities of data for proper training, for example datasets which have many millions of images, rather than just thousands.

However, it is also necessary to consider another taxonomy of neural networks, based on what they are intended to do and how data flows through them. For image processing or classification tasks, the most commonly used neural network types are **Convolutional Neural Networks** (CNNs).



Sample CNN architecture[32]

It should be noted that within the CNN there are three typical layers we need to explain — the **convolutional** layer, the **pooling** layer, and the **fully-connected** layer.

The **convolutional layer** is the key part of the CNN,[33] where most of the computation happens. It consists of three components: the **input data**, the **filter** (or kernel) and the **feature map**. **Input data** can, for example, be a colour image made up of pixels in three dimensions: height, width, and depth in RGB (a value combination of red, green and blue to get a wide variety of different colours).[34]

The **filter** is a feature detector, which is based on a two-dimensional or three-dimensional matrix with specified values (corresponding to the three dimensions of the input) and used to perform a convolution — the mathematical operation for merging two sets of information. The filter moves across the image part by part and multiplies the pixel values it finds with the matrix, writing the result it receives in the **feature map**. Since there are multiple filters in CNNs, each one produces a different feature map. These are stacked on one another to produce the **output of the layer**. The process is repeated for each convolutional layer in the network.[35]

Within the **pooling** layer, the input goes through a similar filtering process as in the convolutional layer. The difference, however, is that pooling is used to reduce the parameters of the input for the neural network to handle compressed information.[36] In order to achieve this, an aggregation function is applied with the filter for each part of the image, which can be either **max pooling** (only the pixel with the maximum value is extracted for the output) or **average pooling** (the average value of pixels is extracted for the output). The process creates summarised versions of **filtered feature maps** which provide stability to the CNN, ensuring it will work correctly even when there are slight fluctuations.[37] Finally, the **fully-connected layer** performs the final classification of the image based on the results it receives from the previous layers.[38]

The deep learning processes that are constantly running in today's information landscape require not only possession of massive amounts of data for training, but also a very advanced technical infrastructure on which to test and deploy neural networks, and human capital in terms of scientific and research expertise. In terms of required resources, it is therefore implied that most of these processes are controlled by a small group of powerful private actors, such as Google[39] and Microsoft.[40]

These powerful tools, powered by information about our world and about us as human beings, are used for information compression, i.e. as means of extracting as much information and knowledge in the smallest number of steps using the least amount of resources (such as minimising computer processing power or human working hours).[41] In the context of policing and investigating crimes, the laborious process of sifting through potentially thousands of hours of video-surveillance footage by hand — or more accurately, by screen and keyboard — conducted by police officers and analysts is incomparable to capabilities AI has to offer. As one article from the World Economic Forum's website puts it, "machines don't suffer from monotony or fatigue".[42]

To discover the location of a crime suspect or determine who could be a potential threat to public safety, law enforcement officers may look at smart surveillance systems as a perfect tool to achieve maximum efficiency. However, this utilitarian, resource-efficient approach to solving complicated social problems applies a machine-interpreted social reduction that doesn't guarantee a crimeless and perfectly safe society. Nevertheless, it places the entire community in a state of permanently reduced level of human rights.

Consequently, we can see that the financial interests of developers frequently align with political interests in perceived efficiency. This has led to the widespread adoption of infrastructure for "safe/smart city" endeavours or similar digitised public surveillance projects around the world. These efforts require public procurement deals to purchase, install and maintain the equipment necessary to power the "smart" surveillance. This usually consists of various devices, such as different types of cameras (e.g. pole-mounted, vehicle-mounted, body-worn, etc.), hand-held smartphone-like devices, as well as data storage and processing units, on which the whole system runs behind the scenes.[43] In the next section, we shall take a closer look at the basic components of such systems, some of the key vendors, and the capabilities of their products.

INFRASTRUCTURE AND SOLUTIONS

CAPABILITIES AND POTENTIALS OF FACIAL RECOGNITION PRODUCTS

ELEMENTS AND DESIGN OF A FACIAL RECOGNITION SYSTEM

According to Deloitte, the global facial recognition market is expected to be worth around 8.5 billion US dollars by 2025, a significant rise from 3.8 billion recorded in 2020.[44] The sheer number of surveillance cameras installed by both public and private entities has normalised surveillance so much that many people now willingly equip their homes with camera systems, believing that it will keep them safer. In a paradoxical turn, this can

lead to increased privacy and security violations, as the recent ransomware attack claim involving Amazon's Ring cameras has shown.[45] Additional privacy and data access issues arise from the fact that in purported "emergency instances" Amazon provides US law enforcement bodies with direct access to Ring camera videos without a warrant, and most users are unaware of that.[46]

Modern surveillance systems, particularly those used for surveillance of public spaces, require a technical infrastructure that is only partly visible to the people surveilled. Observable elements include various types of street-level cameras, sensors and other end-point devices installed or used in public, such as mobile hand-held terminals. However, their visibility is often obscured through urban design practices or by a simple social normalisation. The completely invisible elements that are critical to the systems' operation are various data processing and storage devices with advanced analytics capabilities held hidden from public view. These invisible elements further entrench the power imbalance between "The Watchers" and "The Watched".

Drones are a good example of why devices that capture faces or other input data can be so concerning. As the Electronic Privacy Information Center (EPIC) explains, drones are a privacy threat because of several factors: they greatly reduce the cost of surveillance, make aerial surveillance easy to operate, and can be outfitted with various surveillance add-ons, such as high-resolution cameras, thermal or movement detection sensors. There are also no well-established privacy protections when it comes to aerial surveillance, at least not in the US.[47]

Although drones can sometimes be seen in the air, they are at times completely invisible to humans, especially if flying at high altitudes. Trevor Paglen's art piece "Untitled (Reaper Drone)" shows exactly this — a drone is nothing more than a barely visible, tiny speck on a photograph of a luminous sky, making its way from a US military base to fulfil its mission somewhere on the other side of the world.[48]

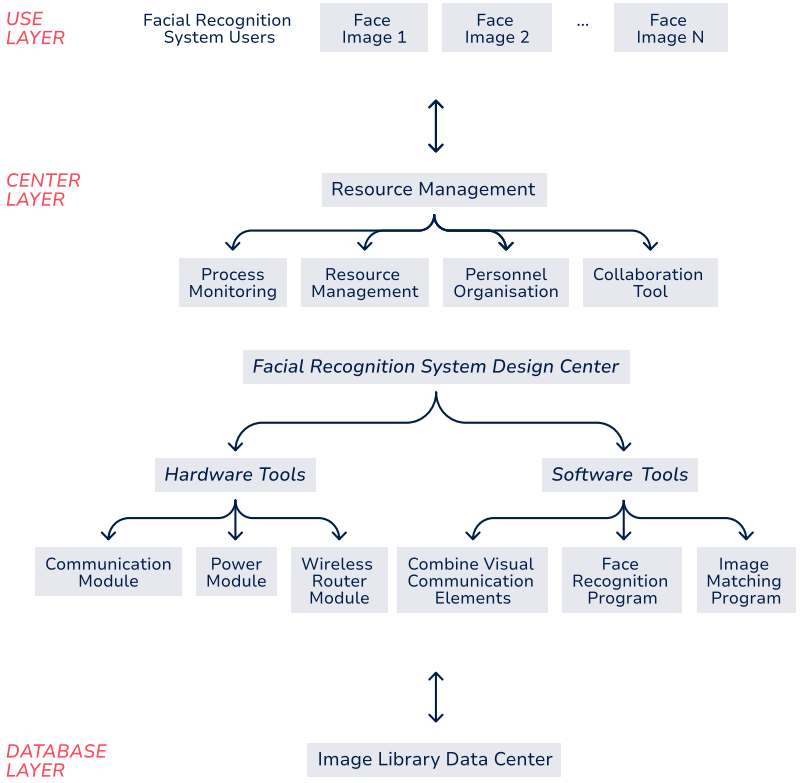
The technical biometric surveillance apparatus is mostly visible from its final or endpoint layer, i.e. the CCTV cameras that people can see in an open space (a square, an intersection, in front of an important building) or in a closed space such as an airport or a metro station. When designing a surveillance system, however, it takes much more than just installing cameras in specific places — careful planning, connectivity, storage and

other supporting resources are just as important. Usually, there are several key elements of a video surveillance system:[49]

- **Cameras**: there are many different types available based on their mobility (i.e. whether they are fixed or portable), their image output type (e.g. colour or black and white), their resolution (standard or high definition) or type of signal, which may be internet protocol (IP) based or analogue (older models);
- **Connection**: like types of signal, connections to the system can be analogue, but the prevalent type used for modern surveillance systems is IP-based. In other words, video output can be sent via a wireless network or through cables, depending on the use case and the infrastructure;
- **Video management and storage**: devices such as digital video recorders (DVR), network video recorders (NVR), or computers/servers with appropriate video management software (VMS) installed are used for managing and storing recorded video. There are also several storage options: internal within the video management devices, external memory units (e.g. hard drives), networked storage (e.g. cloud solutions), or on-board memory on cameras through the use of SD cards, for example;
- **Video analytics**: software solutions providing numerous options to get the most information out of the videos, ranging from identifying a perimeter breach, counting people, performing vehicle licence plate recognition or facial recognition;
- **Viewing devices**: the video feed can be watched on-site directly from a management device, remotely from a system-connected device (computer, mobile phone), or on a video-wall, which is typical for state-of-the-art analytics centres, where analysts can watch feeds from hundreds or even thousands of security cameras simultaneously.

However, this is not the only way to think about the components of a facial recognition system. While examining the design of a facial recognition system as a logical framework, Xuhui Fu divides its architecture into three layers: the **use layer**, the **central layer** and the **database layer**. The **use** layer is employed to send instructions to the system according to the needs

of a person operating the system, e.g. to search for a match of a specific face. The role of the **central** layer is to perform the recognition process and return the information to the user layer, while the **database** layer is used to collect facial image information and provide the system with data required to perform facial recognition.[50] Fu presents this architecture in a diagram:



X. Fu: Diagram of the architecture of a facial recognition system[51]

Obviously, the pivotal steps for facial recognition occur in the video management and analytics elements. CCTV systems of the past, with old analogue cameras recording grainy black and white low-resolution video were not demanding in terms of technical infrastructure and setup, yet still adversely affected human rights. With today's IP-based system capabilities — cameras that can record high definition video even in poor lighting

conditions, massive storage capabilities, and advanced analytics software and hardware — the capacity for biometric mass surveillance raises the stakes to a much higher level.

Once they are approved, installed and tested in a specific context or environment, these surveillance systems are very hard to remove. An example of this is the use of facial recognition in Moscow, which went through a purportedly experimental phase during the 2018 Football World Cup. A similar scenario may be expected in France, where in March 2023 the National Assembly passed legislation authorising the use of AI-powered surveillance to allegedly increase public safety during the Paris 2024 Olympic and Paralympic Games, allowing for experiments at public events in the run-up to the Games.[52]

The flexibility of the design and the variety of products and services available makes the implementation of a smart video surveillance system relatively easy for actors possessing financial, technical and other resources, such as state bodies.

KEY VENDORS AND PRODUCTS

The very lucrative global market for facial recognition encourages the constant development of new products and services, offered by many companies from different parts of the world. However, several vendors of this technology hold powerful positions in the current landscape.

A prominent place is held by **Huawei**, the tech giant that has been under fire in recent years due to its ties to the Chinese government, and an alleged role in the espionage of several Global West nations.[53] This company was one of the main players in the Chinese tech expansion throughout developing countries, most notably in Africa and Latin America,[54] granting it a significant role in the geopolitical and diplomatic conflict between China and the US and its allies.

From a wide range of Huawei products, what stands out most when it comes to AI is the Ascend 910 processor, launched in 2019 and marketed as "the world's most powerful AI processor".[55] These processors are installed in Huawei's advanced AI-focused hardware products, such as the Atlas 900 PoD AI cluster basic unit, whose product page states that it is used for "deep learning model development and training scenarios" and presents it

as "an ideal option for computing-intensive industries, such as smart city, intelligent healthcare, astronomical exploration, and oil exploration".[56]

Huawei also offers the Atlas 900 AI Cluster, a more complex product unit which consists of thousands of Ascend 910 processors, and claims that it has a computing power equivalent to 500,000 desktop computers, capable of completing model training based on ResNet-50 in 60 seconds.[57] ResNet-50 (Residual Network) is a type of Convolutional Neural Network (CNN) with 50 layers developed by a group of researchers in 2015.[58] Given that its performance on a CNN is presented by Huawei as one of its selling points, it is safe to assume that the product is primed for developing computer vision solutions, such as facial recognition.

Huawei has also been a key player in the "safe city" market, a combination of purported urban public safety infrastructure and hardware/software products with advanced ("smart") capabilities. Researchers at the Center for Strategic and International Studies (CSIS) have found that Huawei's "Safe City" offer usually covers a wide range of products and services such as command centres, CCTV cameras, intelligent video surveillance, facial and vehicle licence plate recognition technology, and crowd monitoring. According to CSIS findings, common characteristics of markets where Huawei Safe City agreements are usually made is that they are middle-income, non-liberal countries in Asia and Africa.[59] On its website, the Chinese tech giant also describes what its smart city products offer: "... intelligent recognition technology built into cameras themselves, with front-end recognition capabilities carrying out facial recognition of everyone captured on video and analysing specific behaviours to perform real-time crime prevention."[60]

One of Huawei's "Safe City" projects has been initiated in Belgrade, the capital of Serbia, a Western Balkans nation currently negotiating EU accession. A case study of Huawei's "Safe City" solutions in Belgrade revealed a "test run" in the city conducted by the Serbian Ministry of Interior. However, the page was taken down from the company's website,[61] shortly after, the SHARE Foundation, a digital rights non-profit based in Serbia, published an analysis of the case study which provided more information about the announced smart video surveillance system in Belgrade.[62] Huawei claimed that the test network "successfully verified multiple key functions, such as video retrieval, video compression, automatic licence plate recognition, behaviour analysis, facial recognition, and video quality diagnosis" to the satisfaction of the Ministry of Interior officials. The case

study also mentioned OceanStor, Huawei's high-end storage device, which is used to store the video materials and has the capability to store video content management analysis data for up to one year.[63] This case will be further explored in the Orwellian National Security section of Chapter 3 on Practices.

Another Asia-based facial recognition technology vendor worth mentioning is **NEC**, a Japanese electronics giant offering a wide range of products. The company prides itself on its facial recognition technology being ranked first on the US National Institute for Standards and Technology (NIST) vendor tests to assess technological capabilities and standards.[64]

In April 2019, the company announced its AI and Human Rights Principles, with the aim to "further strengthen NEC's efforts to demonstrate respect for privacy and human rights in relation to the application and utilisation of AI and biometrics data across all businesses."[65] NEC adopted the following principles: Fairness, Privacy, Transparency, Responsibility to Explain, Proper Utilisation, AI and Talent Development, and Dialogue with Multiple Stakeholders.[66] Given the role of NEC in the development and supply of biometric surveillance products, adopting such principles may be a good step in terms of corporate governance. Though such policies can be helpful for internal purposes, they are ultimately driven by and designed to serve commercial interests and do not replace robust legislation. This is especially pertinent given the association of biometric surveillance technology with serious human rights risks, which the Principles do not address.

NEC has supplied biometric surveillance technology to several EU Member States. According to a 2021 report for the Greens/EFA group in the European Parliament, NEC biometric surveillance technology was procured by authorities in Romania, Hungary, Italy, Portugal and Lithuania.[67] Outside Europe, in March 2022 it was announced that Brunei, a small South Asian nation, received NEC's facial recognition product NeoFace Watch, which has been installed at the Brunei International Airport. This was a seemingly free contribution by the Government of Japan, made through the United Nations Office on Drugs and Crime (UNODC). The installation of these facial recognition systems in Brunei was initially discussed with the Japanese ambassador in 2019.[68] The expansion of NEC products to markets such as the EU is somewhat predictable, as Japan has been a long-time political and military ally of the nations of Western Europe and North America, especially the US. Concurrently, its foothold in South Asia from the Brunei example may be perceived as regional tech diplomacy.

One of NEC's facial recognition products, NeoFace Watch, works by "integrating face matching technology with video analytics input".[69] It is a web-based application that is customisable, can be integrated into existing security solutions, and has the ability to process both live and archived video materials (for performing live and retrospective facial recognition).[70] The company's marketing materials further suggest that NeoFace Watch can be used as a flexible facial recognition solution for stadiums, event venues and public transportation.[71]

Out of several major American corporations in the biometric surveillance market, we first turn to **Amazon**. Its most famous product may be the Amazon.com e-commerce platform, but over the years, Amazon has expanded its service portfolio to also become a very influential cloud infrastructure provider with Amazon Web Services (AWS). For example, one of their first data centres (buildings where servers and related equipment are located), which opened in 2006 and is widely relied on for internet services globally, is located in the US state of Virginia. As Ingrid Burrington notes: "Before I knew northern Virginia as the heart of the internet, I knew it as spook country — that is, home to a constellation of intelligence agencies and defence contractors", which seems to be no coincidence.[72] Today, AWS offers a diverse range of data centre and infrastructure locations for its services, with more than 30 geographic regions as of April 2023, serving over 200 countries and territories, i.e. spanning practically the whole world.[73]

As a versatile platform for cloud storage, AWS offers its customers the possibility to use Amazon Rekognition, the company's advanced computer vision service. Given the fact that it runs on AWS, Amazon Rekognition can be applied as a very convenient facial recognition solution and integrated with an existing surveillance infrastructure (e.g. a CCTV system). A Washington Post report from 2019 highlighted how a local police force in Oregon used Amazon Rekognition in their investigations: "Almost overnight, deputies saw their investigative powers supercharged, allowing them to scan for matches of a suspect's face across more than 300,000 mug shots taken at the county jail since 2001."[74] In 2020, Amazon announced that the company was introducing a one-year moratorium on the police use of the Rekognition tool, following high profile cases of wrongful arrests of Black men.[75] In May 2021, the company confirmed it would extend its police moratorium for Rekognition until further notice.[76] However, there has been no public information about what decisions were taken as a result of this move, which calls its credibility into question.

Amazon Rekognition can analyse images and video in order to identify objects, people, text, scenes and activities, as well as to filter purported inappropriate content.[77] There are two Amazon Rekognition application programming interfaces (API), i.e. a set of rules used to enable different applications to communicate with each other.[78] The two APIs are Amazon Rekognition Image, used for analysing images, and Amazon Rekognition Video for video analysis.[79] This essentially means that anyone can develop an app for their purposes and integrate it with the Rekognition service through an appropriate API in order to use the options it provides.

Another US-based company, **Microsoft**, is also worth considering in the context of biometric surveillance technology. A tech giant of old, Microsoft is actively involved in the research and development of AI, as well as updating its corporate governance. In December 2018, the company issued six principles to guide its development and deployment of facial recognition technology. They are Fairness, Transparency, Accountability, Non-discrimination, Notice and consent, and Lawful surveillance.[80]

Similarly to Amazon, Microsoft offers an advanced cloud computing platform called Microsoft Azure, which has more than 200 products and services used to build, run, and manage applications. The company claims that 95 percent of Fortune 500 companies use Azure and that it can cover the needs of various sectors, from government, healthcare, retail, and financial services to manufacturing.[81]

One of the services offered within this portfolio is called Azure Face, which "provides AI algorithms that detect, recognise, and analyse human faces in images."[82] As a cloud-based product, Azure Face is very similar to Amazon Rekognition in terms of how Microsoft's customers can engage with it, i.e. through various APIs based on the intended product usage. The options Microsoft highlights on the Azure Face service description page are face detection and analysis, identity verification, find similar faces, as well as the "group faces" option (i.e. extract a smaller group of similar faces from a set of unknown faces).[83]

In recent years, Microsoft has been keen to show that the company is following a path of vigilance when it comes to the use of their AI-based products and services, especially those associated with high risks for human rights. On the Azure Face service description page, there is a warning that starting June 11, 2020, Microsoft does not sell facial recognition technology to US police forces, and will not do so until there is robust, human rights-

based legislation regulating the use of such technology — although, as with Amazon, there have been no public disclosures of what this means in practice. It is presumable, furthermore, that the company intends to continue selling facial recognition to US police forces at a point in the future.

In June 2022, Microsoft unveiled their framework for building AI systems in a way that they deem acceptable: the Responsible AI Standard. In the official announcement, the company claimed it is limiting access to facial recognition services to a narrow set of customers ("managed partners"), prescribing what they consider to be acceptable use cases. For example, it was specifically pointed out that for Azure Face, Microsoft will be retiring capabilities that infer people's emotional states and identity attributes such as age, gender, smile, face or hair.[84]

Another company statement detailing Microsoft's responsible AI plans, also from June 2022, explicitly introduces the obligation for new customers to apply for access to facial recognition operations in the Azure Face API, Computer Vision and Video Indexer. Existing Microsoft clients were given a one-year deadline (ending June 30, 2023) to apply for access and receive approval so they could continue using these services. On the other hand, face detection capabilities — those that recognise a face but do not ascribe a specific identity — are to remain generally available.[85] Though these steps may seem positive, they give a private company the arbitrary power to open and close the gates for the use of a controversial technology, despite its huge consequences for society.

In order to provide more clarity on what constitutes acceptable use with limited (i.e. restricted) access, Microsoft has provided explanations for the use cases of Azure Face in both private and public sectors. Approved "limited access" commercial uses include "facial verification for identity verification to grant access to digital or physical services or spaces", "facial identification for touchless access control", "facial identification for personalisation", and "facial identification to detect duplicate or blocked users".[86] By comparison, in 2019 the Netherlands' data protection authority warned that under the EU data protection law, using facial identification for access control for anything less serious than securing a nuclear power plant would be an unjustifiable intrusion on people's data protection rights.[87]

When it comes to law enforcement purposes and criminal proceedings, Microsoft defines acceptable uses largely for identification, such as those relating to "prosecution or defence of a criminal suspect who has

already been apprehended, to the extent specifically authorised by a duly empowered government authority in a jurisdiction that maintains a fair and independent judiciary" or assistance in prosecution of abuses of international law. Additional listed purposes are responding in emergencies which pose imminent risk resulting in death or serious bodily injuries, providing humanitarian aid, identifying missing or deceased persons, or victims of crimes.[88]

Microsoft has also published additional consideration for the acceptable uses of the Azure Face service, noting that the company policy globally prohibits the law enforcement use of live facial recognition technology on mobile cameras, such as body-worn or vehicle dashboard cameras, to attempt to identify persons — but not its retrospective uses, despite equal capacity for harm. The company also provides guidance advising their customers on the technical considerations for using the service in public spaces.[89]

Whilst it can seem that companies like Microsoft and Amazon are taking their commitment to due diligence and human rights seriously, it is important to remain cautious about their claims. The use of biometric systems in the provision of humanitarian aid, for example, has received criticism for being one of the most coercive and dangerous uses, putting already vulnerable people at even greater risk of harm.[90] And the use for identifying suspects of crime can easily be a pretext for legalising widespread surveillance, as warned by the EU's top data protection regulator.[91]

There is also the broader question of the suitability of corporate self-regulation. By relying on principles and limitations designed by private companies, the uses of biometric technologies are by definition tied to their interests — instead of being driven by democratic rights and principles. It allows these commercial entities to determine if and how state authorities like the police or judiciary use technology, giving them enormous levels of power. And it may also create the false impression that governmental regulation is not needed, because the companies have dealt with all issues themselves.

Finally, the European Union representative we will cover for the end of this section is the **Thales Group**. Headquartered in France, Thales provides products and services to a wide range of industries, including aerospace, defence and security, digital identity and security, ground transportation, and space.[92] The company is focused on biometric technology and solutions, covering common types of biometrics, i.e. fingerprints, facial

and iris recognition. It claims to have done more than 200 deployments in 80 countries, as of April 2023.[93] In its paper on designing an ethical, socially-accountable facial recognition system, Thales claims that the company designs its solutions in accordance with ethical rules, which are confidentiality and consent, transparency, precision and reliability, security, ethics and compliance, and accountability.[94] The same concerns apply as previously discussed in relation to Microsoft and Amazon.

The Thales Facial Recognition Platform (FRP) is described as an advanced solution which uses a "world-class algorithm based on deep neural networks" for face detection, tracking and recognition. One of the features highlighted by the company is that the FRP can be integrated with different third-party solutions, such as border management, video surveillance, access control, etc. FRP-based applications can also be built through the use of APIs or developed as standalone software. Also, FRP versatility means it is suitable for multiple platforms and environments and can be deployed on a PC, cloud, or mobile device.[95] Notably, many of the use cases listed by Thales have been the subject of intense scrutiny in Europe, with civil society groups calling for prohibitions on the use of facial recognition and AI systems, inter alia, for identification in public spaces and in border management.[96]

What is also specific to this software product is that it contains several modules, each of which is adapted to a specific biometric surveillance scenario. For example, Thales says that FRP Watch can be used to identify individuals in live video streams, coming from hundreds of cameras in parallel through a video management system. FRP Search Expert is intended for forensic investigations focused on finding individuals from databases of photos or videos with advanced face editing features, while FRP Mobile enables facial recognition capabilities for Android devices. In addition, there is a FRP Software Development Kit (SDK) at the disposal of customers, who can use it to develop their own standalone applications with facial recognition that can work both on photos and video materials.[97]

The advanced and extensive nature of the facial recognition technology market means that, in the event that one particular vendor or technological product is not available to law enforcement bodies, for example, they will be able to obtain other similar products whose vendor does not deny service. Some advanced tools, such as those offered by Clearview AI, are even marketed for use by law enforcement and government agencies specifically.

Again, it is important to stress that issues of biometric surveillance abuse affecting human rights on a large scale cannot be left to companies to solve with their self-imposed rules and policies, especially taking into account their profit-driven actions and agendas. For example, in 2020 European Digital Rights (EDRi), a network of organisations advocating for the protection of human rights in the digital environment, wrote to the CEO of IBM asking for an explanation of the company's announcement to "sunset" its "general purpose" facial recognition on the grounds of "justice and racial equity". However, IBM's responses did not provide anything of substance and suggested that they were more focused on public relations rather than human rights issues at stake.[98]

PRODUCT CAPABILITIES

Having described the basic concepts behind the technology underpinning biometric surveillance, such as machine learning and computer vision, we can now focus more on the specific functions and applications of these tools. It is important to understand the capabilities of some commonly used tools, as abuses are facilitated by the very design of these technologies, in addition to the legal and social contexts in which they are deployed.

Many of the tools that are described in the following sections have long been presented, at least by the companies developing them, as not processing biometric data — for example to reassure the public that the systems are compliant with regulatory frameworks that restrict the processing of personally identifiable data. However, the upcoming examples clearly demonstrate that the unique identification of an individual is not necessary for these systems to cause serious harm, such as by perpetuating stereotypes and discrimination. In addition, given the data that these systems are processing about people's faces and bodies, there are strong arguments to be made that such data *should* in fact be considered to be sensitive biometric data.[99]

Racial and ethnic profiling

One of the most concerning examples of what facial recognition tools are able to achieve can be described as "ethnicity detection", i.e. a function that claims to provide information on a person's probable ethnic background based on their face, skin, or other physical or physiological features.

For example, the "Uyghur alert" option was discovered by the media in a Huawei interoperability report concerning their cooperation with Megvii, another Chinese facial recognition vendor. Originally in Chinese, the 2018 document, named "Huawei Video Cloud Solution and Megvii Dynamic Face Recognition Interoperability Test Report", described how Megvii's facial recognition software performed on Huawei's technical infrastructure.[100] According to the report, which was apparently accidentally published online, Megvii's facial recognition and ethnicity detection tool was successfully integrated into Huawei's services.

This kind of profiling comes as a very serious human rights risk for racialised and minoritised people and communities, especially in China, where there have been extensive international reports of various human rights abuses against Uyghur people, which the Chinese government has consistently denied.[101] When reached out to for a comment by IPVM, an online publication reporting on video surveillance and similar security systems, Huawei responded that the described report was "simply a test" and that it "has not seen real-world application". Megvii also responded to IPVM that their solutions "are not designed or customised to target or label ethnic groups".[102] Even if true, the development of such capabilities in and of themselves are still just as concerning.

It is also interesting to note that in this case, the Huawei and Megvii combined system used NVIDIA's hardware, specifically their Tesla P4 graphics processing units (GPUs).[103] Hardware manufacturers — such as NVIDIA — therefore also have a significant role to play when it comes to the architecture behind advanced surveillance systems, which are increasingly dependent on deep learning processes. As noted in the previous chapter, deep learning requires huge amounts of processing power, which drives the demand for the high performance chips that are required for high-end hardware components such as graphics cards (GPUs).

Emotion recognition

Another deeply problematic capability is the purported recognition of perceived emotional states of individuals, usually dubbed "emotion recognition". This is a very dangerous possibility in terms of targeting people, who may be recognised as "angry", for example, and branded as harmful to society and social order.

Public surveillance methods that are based on machine interpretations of a concept as sensitive and elusive as human emotion can force people to present only socially acceptable behaviour when in public spaces. Such induced behaviour in turn leads to an artificially "cohesive" and "happy" society. The foil to this artificial behaviour is that any kind of different personal trait or political or social viewpoint that stands out from "normality", i.e. "average" appearance or behaviour, might be suppressed and oppressed if manifested in public.

On the Amazon Rekognition explainer page, the company claims that the service can interpret "emotional expressions (like happy, sad, or surprised), [and] demographic information (like gender or age)" from facial images.[104] The guidelines state that for each attribute, a confidence score is provided in percentages, e.g. the system can provide an 85% probability that a person is "female" and a 90% probability that they are "happy". Amazon, however, notes that Rekognition shouldn't be used to make these sorts of determinations.[105] This is a meaningless and disingenuous safeguard, as it cannot prevent anyone from using the product in such a manner, and in fact is likely to encourage this, since such tools are specifically designed to make these predictions.

A 2018 blog post from Amazon, responding to a test run of the Rekognition tool by the American Civil Liberties Union (ACLU) states that the default confidence threshold for Rekognition is 80%, which they deem as "good for a broad set of general use cases... but it's not the right setting for public safety use cases". The blog also claims that Amazon's policy is to "recommend that [Rekognition] customers do not use less than 99% confidence levels for law enforcement matches".[106] Again, we see a corporate actor's intention to "self regulate" technology that can seriously impact human rights, particularly in the context of legal proceedings (i.e. wrongful arrests, convictions and similar legal consequences). Taking into account that minoritised communities are the ones usually on the receiving end of technology-influenced wrongful legal consequences, it raises additional doubt of the justifications for the use of such tools.

Amazon's FaceDetail page provides more information on the possible "objects" — characteristics of a person that can be detected with some probability — such as age range, emotions, smile, facial landmarks and whether a person's mouth is open, all of which can be used to gather additional information.[107] The very reference to people's personal traits as "objects" intended for programming is worrying, reducing them to

mere technical attributes intended for machine processing. As "Emotion" objects, Rekognition allows the following values as valid: "HAPPY", "SAD", "ANGRY", "CONFUSED", "DISGUSTED", "SURPRISED", "CALM", "UNKNOWN" and "FEAR".[108]

Amazon is not the only provider offering services which categorise people by their external appearance and claim to know their inner emotional state. Microsoft's Azure Face service (Detect API) at the time of writing offered similar capabilities, which can "optionally be used to analyse attributes about each face using additional AI models, such as pose and facial landmarks like eye or nose position."[109] Similarly to Amazon's Rekognition, Azure Face can return a number of what Microsoft calls "attributes", i.e. traits such as the presence of accessories (e.g. headwear, glasses or mask), age, facial hair, head pose, gender, but also emotions. The potentially recognisable emotions listed are happiness, sadness, neutral, anger, contempt, disgust, surprise and fear.[110] However, as noted in the previous section, Microsoft stated they will retire the capabilities which are purported to infer emotional states and personal identity attributes such as gender by the end of June 2023[111]

Gender recognition

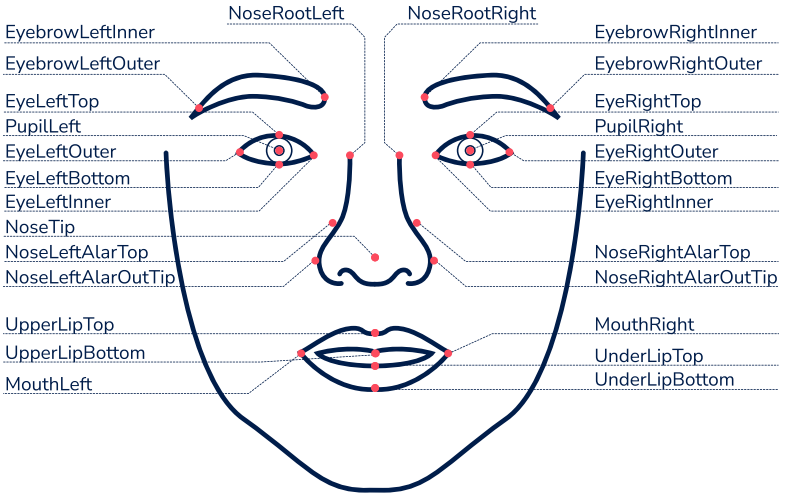
When it comes to gender recognition, this works similarly to emotion recognition on services such as Amazon Rekognition or Microsoft's Azure Face. On Microsoft's Azure service, the possible gender values listed are male, female and genderless, but the page also states that capabilities that predict gender will be retired by the end of June 2023.[112] In the Amazon Rekognition Gender API for example, the possible values the app can return are "male" and "female".

Therefore, at the time of writing, both Amazon and Microsoft offered services with the goal of placing people into boxes based on largely binary stereotypes about gender. Beyond this, however, even if the companies were to provide a broader range of gender identity options, the very premise that people's gender identity is externally observable is at odds with ideas of respect for human dignity and self-expression. From a human rights perspective, it is difficult to see any legitimate use case for using technology to categorise people in this way. More broadly, such technologies are underpinned by a deeply problematic assumption that human identity can be reduced to ones and zeroes — and that this is something desirable.

Amazon states that "gender binary predictions ...[are] best suited for use cases where aggregate gender distribution statistics need to be analysed without identifying specific users" and advises against using gender binary predictions "to make decisions that impact an individual's rights, privacy, or access to services".[113] Yet Amazon's KnownGender API, which allows for the detection of the known gender of a celebrity, functions differently. The values it can return are "male", "female", "nonbinary" and "unlisted", which for some reason allows celebrities a more flexible gender identity compared to the above mentioned categories used for the general population.[114] Again, this emphasises the problems that arise when people's sensitive characteristics are forcibly defined, especially by private companies.

Facial landmarks

As concerns facial features and the recognition of individual people, both Azure Face and Amazon Rekognition rely on detecting the position of facial landmarks. This can also be considered as an intrusive technical capability, given that it reduces recognition to a very granular, micro-level. For example, Azure Face has 27 predefined facial landmarks, i.e. specific points on a face used to identify a person, which are shown on the image below.



Microsoft Azure Face predefined landmarks[115]

Amazon Rekognition has 30 very similar facial landmarks whose position it can detect as possible values.[116] These landmarks essentially describe the key elements used to identify a human face, such as eyes, nose, mouth, chin and eyebrows. As such, the landmarks serve to translate between how machines read faces, compared to how human vision distinguishes between faces.

With systems built with capabilities based on services such as Rekognition or Azure Face, specific shapes and positions of facial landmarks can be sources of targeting and discrimination of people with specific features. This is particularly relevant in scenarios where a specific group or community has been persecuted by the government or is stereotypically connected with supposed "antisocial" or "suspicious" behaviour. We have already seen that a discriminatory capability of biometric surveillance infrastructure, such as ethnicity detection, is very much possible. And we have noted how phrenology or eugenics — both discarded by modern science — can be used by repressive and racist regimes to justify discrimination of people based on the shape of their skull or face. These capabilities of Rekognition and Azure Face could therefore relatively easily be used by their customers for racial or other profiling.

Behaviour and crowd control

Taking into account the possible options that software products offer in terms of biometric surveillance is of course just one part of the story. We must also consider the hardware, i.e. the physical infrastructure such as cameras and supporting devices, which are increasingly embedded with software so that they can perform analyses and issue alerts directly from the device to the computer of whoever installed it. In the example of Huawei's equipment, we can see that the physical components installed and used in public spaces have become a very potent tool for crowd control, behaviour tracking and surveillance of activities such as traffic. Technological developments, which can almost exponentially increase the capacity for surveillance, challenge traditional conceptions of hardware and software as distinct.

Huawei's intelligent video surveillance brochure from 2019 describes several models of cameras. The specification for Huawei M1281-Q, a model with the "Multi-Algorithm Box Camera" label, states that this camera and its integrated software can detect up to 50 objects at once based on intelligent object detection deep learning algorithms — allowing it to target pedestrians, motor vehicles and non-motor vehicles. Judging from the list of features, it seems this camera model is focused on both traffic surveillance

and watching over crowds in public spaces. It is able to detect not only the vehicle licence plates, but also colours, brands, sub-brands, model year and so on.[117]

When it comes to its people-oriented capabilities, Huawei claims that this model can perform person detection and personal attribute analysis, which includes facial attributes, e.g. whether a person is wearing a mask, and predicted characteristics such as gender or age. The camera's shape suggests that it can also be mounted on vehicles, for example police cars. This model also has what Huawei calls "exception detections", meaning that the camera can detect the existence of sound, sudden sound increase or decrease, scene change and loss of focus. What makes it even more interesting is its behavioural and crowd flow analysis. According to the brochure, Huawei's behavioural analysis includes fast movement detection, abandoned object detection, removed object detection, tripwire crossing detection, intrusion detection, area entry/exit detection and loitering detection. The crowd analysis enables functions such as head counting, queue length detection, crowd density detection, crowd gathering detection and heat map.[118] Many of these features are the kind intended to be used at the Paris 2024 Olympics and Paralympics, which is explored in detail in the Practice section.

Another similar camera model with "intelligent" analytics options is the Huawei IPC6284-VRZ bullet camera, which has features including fast-moving object detection, crossing line detection, abandoned/removed object detection, loitering detection, intrusion detection, face detection, colour recognition, and vehicle and pedestrian classification. It is also interesting to note that Huawei gives it a "vandal resistant" seal. In the brochure, Huawei lists two additional camera models, IPC6355-VRZ and C6620-Z33, which are dome-shaped and therefore more suited to watch larger spaces (e.g. squares, intersections, parking lots) from wide angles to cover more area. Both models include the behavioural analysis and exceptions detection features, with the main difference being that the C6620-Z33 is a pan-tilt-zoom (PTZ) camera that can be moved according to the situation.[119]

The proliferation of cameras and analytics that we are seeing in modern CCTV systems requires additional devices and functionalities in order for them to be able to perform their advanced functions as intended. For example, Huawei's NVR800 network video recording devices are designed to coordinate and enhance the AI capabilities of cameras like the ones described. According to its User Guide, the NVR800 supports behaviour

analysis (e.g. motion detection, intrusion detection, tripwire crossing detection and audio diagnosis), target detection, and structured target data extraction, with the "target" presumably being a person or an object such as a vehicle shown in the video stream. The device can also display information like "the occurrence time, frequency, and number of persons in different scenarios". The device also supports the option for PTZ controls on cameras to achieve a wider angle and coverage when necessary. The tagging options makes it easier to pinpoint and even bookmark critical moments while watching live video or playing a recording.[120] Another key function of the NVR800 is that whilst individual cameras can issue alerts, the NVR800 can facilitate a treasure trove of information about each alert — supercharging the surveillance potential of each individual "smart" camera into a veritable panopticon.

When it comes to practical examples of how to use the NVR800 for smart surveillance, Huawei provides an example scenario in which a CCTV system built using this device and Huawei cameras are set up to watch over a residential district. With features such as unauthorised person recognition, mask detection, blocklist-based alerts, target search, and intrusion detection it is possible to have a comprehensive security overview of entrances and exits or open spaces between buildings. For example, the blocklist option works in a way that it "adds images of persons who frequently appear and behave abnormally at the gate of the residential district to the blocklist for alerts". When a banned person appears, an alarm is triggered. Target search enables taking snapshots of all people entering or exiting a building and generates trajectories for the person across a specified period of time, based on the target images, making them easy to track.[121] This description very much resembles a social control scenario, and the mention of mask detection (i.e. whether a person is wearing a mask or not) gives the impression that it is particularly applicable in an event such as the COVID-19 pandemic.

A video analytics function for tracking movement called "people pathing", which is very similar to the one Huawei's products possess, can be performed with Amazon Rekognition Video. This feature enables users to track a path people take in videos and provide information on their facial landmarks, for example, or the location of the person in the video frame at the time of tracking their location.[122] NeoFace Watch, an NEC-developed software product, has a feature called "Flow Analysis", which they say "anonymously monitors individuals and calculates their time-in-queue, providing actionable information about service levels and the

efficiency of operations in aggregate", reminiscent of the crowd analysis options of Huawei's equipment, although their claim of anonymisation is questionable.[123] In addition, the "Video Analysis" feature of NeoFace Watch can process recorded video at "better than real-time speeds" which can be used for the "post-event analysis" of faces and "security review of large-scale disturbances".[124]

All of these features seem to be aimed at public gatherings or large-scale events involving security risks, such as protests, marches, sit-ins or other forms of democratic dissent, as well as public celebrations, festivals and sports events. In earlier days, a typical police force would need to invest numerous personnel and other resources to analyse and track these events. With the introduction of advanced crowd monitoring and behaviour analysis systems, it theoretically becomes easier for police to plan, oversee and potentially react to large groups of people.

In such an environment, protests and various forms of political expression in the streets, squares and other public spaces have become more surveilled than at any point in history. This also represents a paradigm shift from on-the-ground policing, in which persons not charged or associated with a crime will not be further analysed, towards a situation in which every person's identity and behaviour can be analysed, retained and potentially used against them over a long time span. The fact that such biometric surveillance technology is no longer a cautionary tale from repressive regimes, but is now a reality in supposedly open and liberal societies, should make us think about the social values that this kind of technology prioritises. States have a legitimate aim to keep people safe and to enforce the law, just as they have a duty to protect people's liberty and privacy. But once the line of mass surveillance is crossed under the guise of security, it can be a turning point for any society, one camera at a time.

SERVICE-BASED SOLUTIONS

In addition to the tools we have described, which require at least some level of adjustment to existing systems, there are also solutions provided as an end-user facial recognition service. For example, an entity purchasing access to a specific service, such as Clearview AI, uses a platform which is entirely controlled by the service provider, similarly to when a user creates a social media account.

Clearview AI, a US-based company providing the online service of the same name (a sort of search engine for faces), has caused much controversy ever since it was introduced. Because of its data collection and processing practices, Clearview AI has already come under scrutiny of several regulatory bodies from around the world. The UK's data protection authority, the Information Commissioner's Office (ICO), issued a 7.5 million pound fine to Clearview AI in 2022,[125] while France's CNIL went with an even higher fine of 20 million euros that same year.[126] The Italian Garante Privacy later issued an additional fine of 20 million euros.[127] Clearview AI is not believed, however, to have responded to any of the decisions or fines issued in Europe, leading to the CNIL issuing an additional penalty fine of 5.2 million euros in May 2023.[128]

Furthermore, in a joint investigation, the results of which were published in early 2021, the Office of the Privacy Commissioner of Canada and the data protection bodies of three Canadian provinces — Alberta, Quebec and British Columbia — found that "Clearview engaged in the collection, use and disclosure of personal information through the development and provision of its facial recognition application, without the requisite consent."[129] However, probably its biggest regulatory hit to date happened in 2022 in the USA, where the American Civil Liberties Union (ACLU) mounted a successful court challenge under the Illinois Biometric Information Privacy Act (BIPA) against Clearview AI, in order to prevent the company from selling its faceprint database to businesses and private entities anywhere in the United States.[130]

What is specific to Clearview AI is that its facial recognition tool is based on photos automatically collected (scraped) from the internet, particularly websites where people post a lot of photos of faces, such as social media platforms. Clearview AI CEO Hoan Ton-That's statement that as of March 2023 the company collected about 30 billion facial photos from the internet sounds staggering, as it is most likely the largest privately-owned facial photo database currently in existence.[131] This makes usual police photo databases practically obsolete, especially since Clearview AI markets its service towards law enforcement. On the company overview page, Clearview AI states that they have developed "a revolutionary, web-based intelligence platform for law enforcement to use as a tool to help generate high-quality investigative leads".[132]

In response to the use of Clearview AI by Swedish police — reportedly one of eighteen European law enforcement agencies to do so, including Spain, France and Serbia[133] — the Swedish data protection authority, the IMY, also took action against Clearview AI.[134] However, unlike DPAs in Italy, France and the UK, it is interesting to note that the IMY's action was taken directly against the police for their unlawful use of Clearview AI, amounting to a 250,000 euro fine, rather than against Clearview AI.

Although there is much controversy surrounding Clearview AI and how it uses the personal data of practically anyone who has ever appeared on the internet, there is also a lack of transparency when it comes to the technical process of how their tool actually works. Based on publicly available information and their own expertise on the matter, a privacy activism group called None of Your Business (NOYB) tried to break down the steps of how Clearview AI's service operates in a complaint submitted to the Austrian Data Protection Authority:[135]

- In the first step, an automated image scraper scours all public webpages and searches for any images likely to contain a human face. In addition, the scraper also collects any metadata associated with the images, such as its link (URL), image title, or the title of the webpage where it was found.
- Then, all these images and associated metadata are stored on Clearview AI server infrastructure and are kept even after the images have been deleted from the original source or made private.
- Image processing neural networks are used to extract unique identifying features of each face and turn them into so-called vectors, i.e. numerical representations that consist of 512 data points.
- The vectors/identifiers (more commonly known as face templates) are stored in a database where they are associated with images and related metadata. The next step is to hash the vectors, i.e. to give them a shorter, fixed-length value or key through a mathematical process, in order to make the database searchable and be able to compare the faces.
- The final step is facial matching, which occurs when a user/customer of Clearview AI uploads a photo of an individual they

> want to identify. The uploaded image is analysed, the face vector extracted and given a hash value, which is then compared to hashes in the database of previously collected images. The user then receives a search result with any matched images, as well as all other metadata associated with them.

In the context of Clearview AI and its enormous capabilities, coupled with regulatory challenges to control its use, we also need to take into account similar facial image search services, one such being PimEyes. PimEyes is a service presented as a "reverse image search" that allows users to upload facial photos and find where the images are located online through the use of facial recognition technology. As explained on its official website, "in the results we display not only similar photos to the one you have uploaded to the search bar but also pictures in which you appear on a different background, with other people, or even with a different haircut."[136]

In November 2022, the UK NGO Big Brother Watch filed a complaint to the UK DPA against PimEyes, claiming that the service unlawfully processes biometric data on millions of UK citizens. As Big Brother Watch noted in their complaint, in addition to providing images, the search results also provide the image URLs, potentially offering additional information about an individual. These functions can put people, especially women and minoritised people, at an enhanced risk of stalking, harassment and violent crimes. The tool was also compared to Clearview AI in terms of having a similar business model.[137] PimEyes responded to the complaint, claiming that it is not nor has it ever been "a tool to establish the identity or details of any individual", adding that the purpose of the service is "to collect information about URLs that publish certain types of images in public domains". PimEyes further claims that the main "targets" of its search engine are not individuals, but public webpages.[138]

In another blog post, PimEyes states that they only provide a tool and that the responsibility for its use lies on the users. The platform also offers an opt-out mechanism, for which the individual has to submit a photo, an anonymised scan of an identification document (ID) and an email address.[139] Absurdly, people have to provide more information to opt-out of data collection that they presumably didn't want in the first place. The fact that the responsibility is shifted on the users does not reduce the intrusiveness of such a powerful tool.

In general, vast amounts of facial data published online became available for the taking thanks to the development of web page scraping tools. It seems that there is a long battle ahead to protect our faces from being digitised and turned into searchable mathematical keys, without sufficient and effective control or oversight. In particular, the global nature of both the internet and services like Clearview AI and PimEyes makes effective enforcement very difficult. This has been emphasised in decisions from several EU DPAs, for example the Italian Garante Privacy demanding Clearview AI to delete the images and other data of all Italians, which does not address the broader structures and systems within which these companies operate. The fact that tools such as Clearview AI keep becoming more and more sophisticated is also disadvantageous for the protection of human rights, particularly in the context of law enforcement use. Your face may not be in a mugshot database of your country's police force, but you can bet Clearview AI almost certainly has it somewhere on their servers.

Things are not completely hopeless though, at least in the European Union, where in May 2023 the Internal Market Committee and the Civil Liberties Committee of the European Parliament voted to adopt a ban on the use of AI for the "indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases" in their draft negotiating text of the Artificial Intelligence Act.[140] This wording very much resembles the basis of Clearview AI's mass data collection and processing practices.

BEHIND THE TECH: DECONSTRUCTING FACIAL RECOGNITION SOLUTIONS

There may not be a lot of transparency when it comes to biometric surveillance solutions and how they work in general, but in order for the companies to protect the essence of their products, they need to patent them before the competition. Therefore, patent information that is publicly available and searchable can provide a significant insight not only into capabilities that current products have, but also the potentials of those that are planned for future development. Although patents are a source of great power in technology-mediated social relations, they are also a window into the tools that entrench these power relations.

VENDOR PATENT ANALYSIS

Most companies developing hardware and software products are filing a large number of patents all the time in order to be competitive, and constantly trying out new methods. Even though patents for many technologies may sound very general and technical, companies often rely on them to protect their right to intellectual property and therefore preserve the value of their lucrative products and services. For example, Amazon's "Enhanced face recognition in video" patent explains how "infrared imaging can be used to determine when a person is looking substantially towards a device, such that an image frame captured at that time will likely be adequate for facial recognition."[141]

It is interesting to see that developers and companies are working on ways to improve the process of facial recognition and therefore add more value to their products, especially since patents expire. Amazon's patent description, for example, further explains that since analysing video information can be very resource-demanding in terms of processing power and energy, it is instead more desirable to analyse only certain portions of the captured video, including on mobile devices. In particular, this patent seeks to overcome

the challenge posed by a user or subject not always looking directly at the camera, or the occurrence of blurring due to movement.[142]

In the context of Ring cameras and the direct access to footage by law enforcement agencies, it is interesting to note that Amazon has patented technology for sharing video footage for parcel theft alerts. The patent, called "Sharing video footage from audio/video recording and communication devices for parcel theft deterrence", suggests that using doorbell cameras like Ring "can also aid in crime detection and prevention".[143] The device is essentially configured to watch for parcels in the drop-off zone and share a signal when a theft is likely to have occurred, by sending an alert to at least one law enforcement agency. Also, the system can use facial recognition on the recording to determine whether the person removing the parcel was authorised to do so.[144]

To tackle the challenges from large quantities of facial images that may contain same or similar faces, Microsoft secured a patent to enable the grouping and ranking of images based on facial recognition data. This works by first determining facial recognition data for each face detected in each image and comprises a face identifier that uniquely identifies each face. The system generates a set of facial feature descriptors and a face score based on the state of eyes and mouth (i.e. if they are open or closed). This is used to indicate the overall quality of each face image, as well as to produce a face "signature" that uniquely identifies the individual.[145] The process of "grouping" is performed according to face signatures and face scores, so that images of the set are put into one or more groups. These groups are made up of one or more images that each show a detected face that represents the same person as the one represented by any other detected face shown in any image in each group.[146]

Microsoft has also patented technology for face recognition in video content, which is based on face galleries generated from face detection data in the input video frames. These galleries are labelled and used for recognising faces that appear in the video, and the metadata associating a face with a video frame are generated and maintained for further identification.[147]

Another application of facial recognition for identification can be found in Microsoft's patent titled "Verifying identity based on facial dynamics". As per the description, the technique comprises two components. The first component includes a comparison of newly captured facial data with a "previously stored structural face signature" of the user, while the second

component checks whether the input facial data matches the "dynamic face signature". The novelty of this dynamic face signature is that it "describes movement of parts of the face over a span of time as the user performs a gesture, and the correlation of different parts of the face during the movement". The patent description suggests that this facial movement-based technique is aimed at reducing the risk of malicious actors spoofing the appearance of an authorised user.[148]

To better understand the connection between facial detection and facial recognition, Huawei's patent titled "Adaptive image cropping for face recognition" explains how to improve the process when an image is passed from a face detection neural network (i.e. this is a face) to a facial recognition neural network (i.e. this is who the face belongs to). This process is associated with a bounding box: an area which captures the face. If the face has not been accurately circumscribed by the bounding box, this will lead to errors in the facial recognition network.[149] This approach shows that the use of neural networks is of immense importance to modern facial recognition systems, especially for improving their accuracy and reliability, which are of course matters of economic interest to the vendors.

Patents also offer a window into how companies like Clearview AI will strategically use these intellectual property protections to maintain their market dominance. In January 2022, Clearview AI published a press release announcing that they had been awarded a patent "Methods for Providing Information About a Person Based on Facial Recognition". The press release does not say much about the essence of the technology, only that it was "the combination of gathering information from the public internet with facial recognition capabilities that earned Clearview AI patent protection".[150] When you read through the very detailed patent text, however, it is clear that Clearview AI have gone to significant lengths in order to hold onto their technology.

The invention summary describes the process in the following steps:

- "receiving facial image data transmitted from a user device. The facial image data comprises at least a captured facial image of the subject;
- transforming the facial image data to facial recognition data;

- comparing by a server device the facial recognition data to reference facial recognition data associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image;
- upon identification of the candidate matching the captured facial image, retrieving from the database personal information (e.g., biography, profile information) associated with the candidate; and
- transmitting the personal information to the user device and causing the user device to display the personal information."[151]

The patent description notes that "reference facial recognition data", i.e. the source facial images, are scraped from the "internet, professional websites, law enforcement websites or departments of motor vehicles". It is also mentioned that the "database comprises a plurality of criminal records associated with the facial images stored in the database", probably referencing mugshot and similar databases.[152] When it comes to using the Clearview AI service, the patent explains that "the disclosed system can be operated via desktop or remotely via smartphone, enabling users who conduct criminal investigations, background checks, etc. to instantly establish the identify and obtain biographical data on individuals via one or more facial databases with supplemental links to social media, conventional media, professional websites, etc."[153]

The patent also describes the optional notification if the matched individual is a "person of interest", which may include a missing person, a person accused of a crime or with a criminal record, a sex offender, a person who has suffered memory loss, or a person who they claim "may otherwise pose a high risk to the public".[154] In a chilling aside, the patent description notes that "police may react differently to a person with no arrest record and a medical condition, and a person facially detected to have a history of assaulting police."[155] This seems like Clearview AI's tool is pre-determined to further entrench the power relations that work against oppressed groups, for example Black communities in the USA, who have been well-documented to be targets of police brutality and false accusations of being "aggressive". Highlighting exactly how technology embeds these discriminatory patterns, a 2018 study showed that emotion recognition routinely predicted that Black men were angrier than white men even when their expressions were the same.[156]

In September 2022, Clearview AI announced that their second patent titled "Scalable Training Data Preparation Pipeline and Efficient Distributed Trainer for Deep Neural Networks in Facial Recognition" had been approved. The company stated that the patent was awarded "for its ability to create highly accurate, bias-free facial recognition algorithms from publicly available information", i.e. that Clearview AI is "able to create a data set that represents all demographics with its unique data preparation and distributed training algorithms".[157]

According to the patent, the system extracts faces from raw facial images and it may pre-assign an identity label to the subset of images. These identity labels can be usernames from a public social media website or keywords related to a search engine query. One of the key features of Clearview AI's systems, as described by the patent, is to "ensure that the facial images corresponding to an identity label indeed belong to the identity (intra-identity cleanliness), and there are no other images of the same identity mislabeled as a different identity (inter-identity cleanliness)".[158] This dataset "cleaning" can be achieved with the use of a neural network facial recognition model. But one particularly interesting feature is the possibility of data set image augmentation: "A highly effective approach to increase meaningful variations within an identity is to augment the facial images in certain ways that maintain high fidelity to the natural occurrence of that identity, such as accessories (e.g., glasses, hats, masks), lighting variations, and ageing."[159] This makes it possible, for example, to expand on an existing data set of images and even improve the image database over time as new images are processed and augmented.Although the patents provide some insight into how these technologies work and at least some level of transparency, the key is in the source code, which is kept as a safely guarded business secret. Until there are more code transparency/open source requirements for such invasive systems that enable mass biometric surveillance, we are far away from achieving a level of social consciousness of the dangers these technologies pose for human rights and freedoms. And even if Clearview AI's dubious claim to be free of bias turned out to be true, it would do very little to mitigate the enormous rights violations entailed by their services.

CONCLUSION

Based on the technical aspects of the technology used for biometric (mass) surveillance practices, we can see that in addition to many risks for human rights and freedoms, the design and use of this technology also adds to entrenching systemic social issues such as racial profiling, targeting and discrimination. In particular, many of these tools are designed to mark out "The Other", i.e. people who are perceived as different from the majority population based on their appearance, beliefs or legal/social status. It seems that the pursuit of "averageness" or "normality" in a person based on their physical appearance, as we could see from Francis Galton's work, has only been exacerbated with "digitised bodies" and systems capable of processing this data faster and in larger volume than any human, especially with the advances in neural networks. As machine learning systems require never-ending streams of data in order to be trained, the development of more biassed data sets will keep fuelling the fire of issues posed by mass processing and classification of biometric data.

Massive networks of cameras sprawling entire cities and providing enormous amounts of information on people's appearance, behaviour and movements do not provide a safe space for protests or other forms of civil disobedience. Even the average "nothing to hide" and "law abiding" citizen would become a "walking barcode", ready to be scanned under the watchful eye of biometric surveillance infrastructure. The political turmoil around the world,[160] and more than a decade of global decline of internet freedom,[161] also show that when there is an opportunity to use technological means to control or limit political speech, protests, and other forms of civic organising, political powers in both authoritarian regimes and even those with apparently higher levels of democracy will not hesitate much to seize it.

These rapid scientific and technological changes have expectedly been exploited by private actors with immense resources, high levels of social influence, and effectively no public accountability, except to their shareholders. It is therefore dangerous to leave the respect of human rights to the benevolence, whims, and public relations strategies of powerful corporations as a kind of "self-regulatory" action, as we've seen from the examples of Microsoft and Amazon. Facial recognition and related biometric surveillance technologies are a very lucrative market, and therefore

it is expected that the companies selling them will continue to invest in their development, seemingly without much regard to how their products will actually be used.

Technology is almost always one step ahead of legislation reining it in, no matter how agile today's lawmakers and citizens' representatives are in recognising its adverse effects on society, at least the minority of them that understands the challenges at hand. It is also a matter of geopolitical position and perspective, given that US and Chinese companies are leading the push compared to European ones when it comes to development of facial recognition and other technologies used for mass biometric surveillance. As the European Union pushes towards another landmark legislation aimed at governing our societies in the digital age — the Artificial Intelligence Act — this alone cannot ensure that values of freedom and personal autonomy are preserved. If the push for technologically-driven "security", public order and "social harmony" are prioritised above all else, it could be a point of no return when it comes to the respect of freedom of expression and assembly, the right to protest, as well as privacy in our streets, squares, parks and other public spaces.

Employing intrusive technologies such as facial recognition to make decisions which can produce serious legal consequences for citizens (wrongful arrests or criminal convictions) also poses a serious risk. "Live" facial recognition, i.e. identification of people from surveillance footage processed in real time, gets a lot of attention, but retrospective biometric identification of people from recorded video-materials is not any less dangerous. The case of Mr H, who was convicted of burglary in France only based on being identified with facial recognition from a security camera recording, shows what the legal ramifications could look like as these technologies become even more present. The facial recognition system narrowed the search down to 200 people as potential suspects, and the police singled out Mr H and charged him with the crime, despite a lack of additional evidence to confirm that he was the perpetrator.[162] Pertinently, despite requests from Mr H's lawyer to provide information about how the system came to its prediction, the court found that the intellectual property rights of the provider took precedence. This is a glaring example of why technology cannot be used as an excuse to abandon legal due process, and why the interests of private companies cannot be allowed to prevail over the right to a fair trial and the presumption of innocence.

LEGAL

INTRODUCTION

The legal contexts surrounding the processing of biometric data vary dramatically across the world, with different jurisdictions all having their own definitions for what actually constitutes "biometric data". Thanks to the General Data Protection Regulation (GDPR) and its lesser-known police counterpart, the Data Protection Law Enforcement Directive (LED), the EU is frequently seen as a leader in having laws to ensure the protection of biometric data by strongly restricting, and in some cases prohibiting, its use. However, it is by no means perfect – with enforcement a key site of criticism, and a generally narrow focus on identification use cases. The UK's equivalent framework has failed to stop many harmful deployments.

This research found only two jurisdictions where there have been attempts to regulate the development, deployment or use of facial recognition and other biometric systems specifically (rather than just the underlying biometric data): the US and the EU. At the time of publication, the EU is still grappling with where to draw its line in the sand against biometric surveillance in the landmark Artificial Intelligence Act, with the European Parliament proposing a full ban on all live and most retrospective remote biometric identification in publicly accessible spaces. Meanwhile, various US states have already enacted bans – although only ever for specific sectors or uses, such as police or education, and often with exceptions. Several proposals for a federal-level ban are on the table but none are yet in place.

The almost dozen US states that have chosen to regulate biometric surveillance in some form have overwhelmingly chosen to limit this to facial recognition, implicitly excluding other forms of biometrics. The approaches have varied from a full ban, to moratoria (either for a certain amount of time or until authorising legislation is enacted), to a regulatory framework which lays out the conditions that must be reached in order for a use to be permissible.

In the state of Washington, the legal framework allows the use of facial recognition in the provision of many public services, and has seen speculation that a senior employee of Microsoft had influence over the permissive approach taken. Interestingly, Washington has prohibited facial recognition matches on the basis of a sketch or other manually-produced

images, but allows searches on the basis of a lookalike. There are many similarities between the framework in Washington and the one in Colorado, with a key difference being that Colorado also brought in a task force, which Washington did not find the funding for. It seems, therefore, that the level of oversight is dependent on economic considerations.

Several states show attempts to minimise the risk of abuses. In the state of Virginia, anyone who makes a non-permitted facial recognition search is guilty of a misdemeanour (a criminal charge). And in Maine, there is a requirement to delete any evidence that has been gathered unlawfully. On the other hand, the state of Massachusetts is one of several states that allows the Registry of Motor Vehicles to be used to conduct searches. This seemingly mundane federal agency thus becomes a central point for facial recognition searches in the US thanks to the vast amount of biometric data that it holds.

One important insight from the US is a challenge to the received wisdom that a moratorium is the first step towards a ban. Whilst it is often assumed that a moratorium is a precursor to a ban on facial recognition, the states of Virginia and Vermont show that they are flimsy tools, vulnerable to reversal.

In Canada, a police scandal involving the infamous Clearview AI catalysed a much-needed update of national privacy laws; in 2021, for the first time, biometric data was considered as sensitive data, rather than being treated the same as other data. Now, the country is considering a new law, the AIDA, which will require providers to self-assess whether their artificial intelligence systems are risky or not. Like the Virginia legislation, it creates criminal offences for misuse – with fines and even imprisonment. Whilst Canada's AIDA shares a risk-based approach with the EU's AI Act, it does not, however, contain any prohibitions, raising questions about whether it will have the tools to deal with biometric mass surveillance practices.

Latin American countries have come under serious fire for their treatment of biometrics. Almost two thirds of the region's biometric deployments do not have a legal basis, which has been credited to a general lack of consistent and modern rules to protect biometric data. Brazil, for example, only implemented a right to data protection in 2020. Litigation has been important in several countries in the region, however, with an Argentinian court declaring a Fugitive Facial Recognition System unconstitutional, and the Mexican supreme court doing the same for a national cellphone biometric registry. The Argentine court also recognised privacy and data

protection as collective rights, which is important as the other jurisdictions considered in this book only recognise these rights in a very individual way.

India and China are often pointed to as extreme examples of biometric mass surveillance. In India, legislation is generally focused on enabling deployments rather than safeguarding them, with evidence of several rights-violating police deployments. India also boasts the largest biometric identity programme in the world, which has crept into becoming necessary for people to access bank accounts or phone contracts. In China, police in the capital of Beijing boast of the city's 100% surveillance camera coverage, with drones deployed in Xinjiang to reach where CCTV cameras cannot. Perhaps most notorious in China is the use of facial recognition to facilitate the mass detention of Uyghur people. In recent years, there have been several laws in China that regulate personal data protection generally, as well as regulation that focuses on the use of facial recognition technology specifically. While this regulation seems to be focused mostly on the private sector, there is emerging case law (that concerned use of facial recognition) where courts acknowledged citizens' personal data protection rights.

Another key question raised in this section is the role of technical accuracy standards in facial recognition legislation. The US state of Virginia has mandated that systems must achieve a rate of 98% true positives and India has set this at 80%. However, without knowing how many false positives the system generates, both statistics are close to meaningless.

AUSTRALIA

What type of act regulates processing of biometric data

Data protection law
Yes, the Australian Privacy Act, 1988.

Local level legislation
Yes, on state and municipality levels.

Defining and regulating facial recognition

Data obtained through Facial recognition is defined as biometric data.

Details

Specific use cases defined

- Any sensitive data, including biometrics, can be collected only if there is a legal basis for processing or if the collection of the information is required or authorised by Australian law or a court/tribunal order.
- A law enforcement agency can collect sensitive information if they reasonably believe that the collection is reasonably necessary for, or directly related to, one or more of the agency's functions or activities.

Specific authorities defined

- Yes. The Office of the Australian Information Commissioner serves as a supervisory authority; it can issue opinions and guidance and is responsible for handling complaints; has the mandate to conduct investigations and issue fines.

AUSTRALIA

CONTEXT

The use of facial recognition and other biometric technology by Australian law enforcement agencies is the subject of intense debate between human rights proponents on the one hand, and law enforcement officials on the other. There is still no federal law that would regulate the use of facial recognition and other biometric surveillance in a comprehensive manner. However, Australia does have a Privacy Act that functions as a general data protection law, including regulating the use of biometric data on a broad level. Nonetheless, the use of facial recognition by the police seems to be very present in practice.[163]

As early as 2014, an initiative was put forward to make a single national database containing all the photos from passport and driving licence databases, called the National Facial Biometric Matching Capability (shortened to "Capability" or "NFBMC"), to be used for different facial matching purposes.[164] This initiative was formalised in 2017 when all state and territory leaders signed the Intergovernmental Agreement on Identity Matching Services (IGA), which ought to become fully operational once the appropriate legislative framework is in place, on federal and state levels.[165]

The Capability database is being filled with some data in the states of Queensland, South Australia, West Australia, Victoria and Tasmania, since those states issued legislation that enables such data collection from different state authorities.[166] Even if all the states made local laws that would enable full data *collection* as is envisaged in the IGA, the exchange of data between the states, as well as federal agencies, would still have to be on hold until there is a federal regulation to enable such data *sharing* for facial recognition purposes.[167]

Legislative efforts on the federal level failed in 2019 when the Identity-matching Services Bill 2019 was introduced to the Parliament.[168] The purpose of the Bill was to authorise the Commonwealth (federal government) to facilitate the sharing of identification information, including facial images, between the Commonwealth, states and territories for the purposes of identity-matching.[169] However, this version of the Bill was rejected by the Parliamentary Joint Committee on Intelligence and Security (PJCHR), which found that the Bill has to be redrafted so that the regime for identity matching is built around privacy and transparency, and is subject to robust safeguards.[170] The redrafted version of the bill has not been introduced to the Parliament so far, but there has been no confirmation that the government gave up this legislation either.[171] The Office of the Australian Information Commissioner (OAIC) will be in charge of preparing a privacy assessment in relation to the NFBMC. According to information from their website, the preparation of this privacy assessment is behind due to delays in the enactment of the Identity-matching Services Bill,[172] which might be an indication that the new version of the bill will be put forward by the government.

Even though there is still no legislative framework governing the use of facial recognition by law enforcement, it has nonetheless been used for quite some time now.

According to a statement from a New South Wales police spokesperson, this police force has been using facial recognition technology since 2004, to establish and verify the identities of persons of interest for investigative purposes.[173] On their website, the police provide some information about this practice, referring to the Privacy Act, their local Privacy and Personal Information Act 1998 (NSW), as governing legislation for their use of facial recognition. They have also been public about trial facial recognition projects that were met with public pushback since they raised significant privacy risks due to a lack of appropriate legal safeguards.[174]

South Australia Police have also made statements about their use of facial recognition, claiming that there is no legislative restriction on the use of this technology in South Australia for investigations.[175]

There are also reports that facial recognition might have been used on protesters,[176] and that police used it during the COVID-19 pandemic in trial mode, in order to support quarantine-related measures.[177] In the private sector, facial recognition cameras have been used in supermarkets,

with explanations being that this technology was used to identify persons of interest who have previously been involved in incidents,[178] or in order to understand and improve customers' experience via surveys done on tables that were taking faceprints (images captured via tablet camera were converted to algorithmic faceprints).[179] Several such examples are explored in more detail in the Practice section of this book.

Facial recognition also sparked public attention in 2020, when the UK's Information Commissioner's Office (ICO) and the OAIC launched a joint investigation into Clearview AI's handling of personal information, concentrating on the usage of biometric and scraped data by the company.[180] As will be elaborated further in the case law section, this investigation resulted in the OAIC finding that Clearview AI had breached national privacy laws and must not only cease collecting images of Australians, but also delete existing photographs of Australians in its collection.

In their report from 2021, the Australian Human Rights Commission recommended legal reform to provide better human rights and privacy protection regarding the development and use of biometric technologies, and a moratorium on the use of biometric systems in high-risk decision-making until such protections are in place.[181]

There have also been initiatives from the academic sector to make a model law which would regulate the use of facial recognition more in accordance with human rights standards.[182]

LAW

Australia is a party to the International Covenant on Civil and Political Rights (ICCPR),[183] but there is no federal charter or bill of rights (within the Constitution or otherwise) that would regulate privacy as a human right.[184]

The Australian Privacy Act was enacted at the end of 1988 and became applicable in 1989. It has been subsequently amended several times,[185] while the latest amendments were made in 2022.[186] The Privacy Act covers Australian Government agencies and any organisation with an annual turnover of more than AU$3 million, and other organisations under special conditions regulated in the act (e.g. depending on the sector where they operate). The Act is structured in such a manner as to regulate some specific issues, including the general obligations of relevant stakeholders and rules

around OAIC. At the end of the Act, there are 13 principles contained in its Schedule 1 (Australian Privacy Principles or APPs). These principles are very similar to the principles in GDPR Article 5, in the sense that they provide overarching rules to be relevant for any personal data processing. They are nonetheless more detailed and practical than their GDPR equivalents.

There is no mention of facial recognition specifically, nor are facial recognition templates expressly mentioned in the Act. There is, however, regulation of the biometric templates and the biometric information that is to be used for the purpose of automated biometric verification or biometric identification — both of which are considered to be a type of sensitive information. According to the OAIC interpretation, biometric information includes features of a face.[187]

The rules on the collection and processing of sensitive information are quite general.

According to Principle 3 of the Privacy Act, which regulates data collection, sensitive information can be collected only if there is a relevant legal basis.

A government agency must not collect sensitive information about an individual unless: (i) the individual consents to the collection of the information;[188] and (ii) the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. According to the Privacy Act definitions, consent means express consent or implied consent.[189]

The Privacy Act lists several other situations when the collection of sensitive information would be permissible, even when conditions (i) and (ii) are not met. One such situation is when the collection of the information is required or authorised by or under an Australian law or a court/tribunal order.[190] As explained, there is not currently any other such law authorising or requiring such processing.

For law enforcement bodies there is a special rule. Collection of sensitive information would be allowed if the enforcement body "reasonably believes" that the collection of such information is reasonably necessary for, or directly related to, one or more of the bodies' functions or activities.[191] The standard of "reasonable belief" is what distinguishes enforcement bodies from other regulated entities, including other government agencies. However, such a broad exception may add to concerns that excessive use

of facial recognition and other biometric surveillance by law enforcement agencies increases the risks of mass surveillance and other human rights concerns.[192]

Based on information on the OAIC website, no guidelines have been issued with respect to facial recognition, or more generally, the processing of biometric information.

CASE LAW

In anticipation of the formal rollout of the Capacity, several Australian law enforcement agencies (including the Australian Federal Police, Victoria, and Queensland police) started using Clearview AI's database within their existing facial recognition systems. The government first denied using the company's service, but in early 2020 customer data leaked by Clearview AI revealed that Australian police personnel had in fact been using the service, presumably in an informal manner.

In response to this and other potential violations, the OAIC and the UK's ICO launched their joint investigation into Clearview AI in July 2020.[193]

The next year, in October 2021, the investigation was complete,[194] finding that Clearview AI had breached Australian privacy law.[195] According to OAIC findings, the breaches included: (i) collecting Australians' sensitive information without consent; (ii) collecting personal information by unfair means; (iii) not taking reasonable steps to notify individuals of the collection of personal information; (iv) not taking reasonable steps to ensure that the personal information it disclosed was accurate, having regard to the purpose of the disclosure; and (v) not taking steps to ensure compliance with the Australian Privacy Principles by implementing appropriate practices, procedures and systems.[196]

The OAIC ordered Clearview AI to "cease collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates collected from Australia".[197] However, no monetary fines were imposed.[198]

Later that same year, in November 2021, the OAIC issued another determination establishing that the Australian Federal Police (AFP) failed to comply with its privacy obligations in using the Clearview AI facial recognition tool.[199] Violations were made by (i) failing to conduct a privacy

impact assessment for a high-privacy risk project and (ii) acting in breach of the requirement to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities, as is regulated in the Australian Privacy Principle 1.2.

This OAIC determination directs the AFP to engage an independent assessor to review and report to the OAIC on residual deficiencies in its practices, procedures, systems and training in relation to privacy assessments, and make any necessary changes recommended in the report, as well as to ensure that relevant AFP personnel have completed an updated privacy training programme.[200]

CANADA

What type of act regulates processing of biometric data

National constitution
Yes, the Canadian Charter of Rights and Freedoms, 1982.

Data protection law
Yes, the Privacy Act, 1985; the Personal Information Protection and Electronic Documents Act, 2000.

Bylaws
Yes.

Guidelines
Yes.

AI Regulation
Yes, in development.

Local level legislation
Yes, provincial level.

Defining and regulating facial recognition

Data obtained through facial recognition is defined as biometric data in Quebec.

Data obtained through facial recognition is regulated as sensitive data.

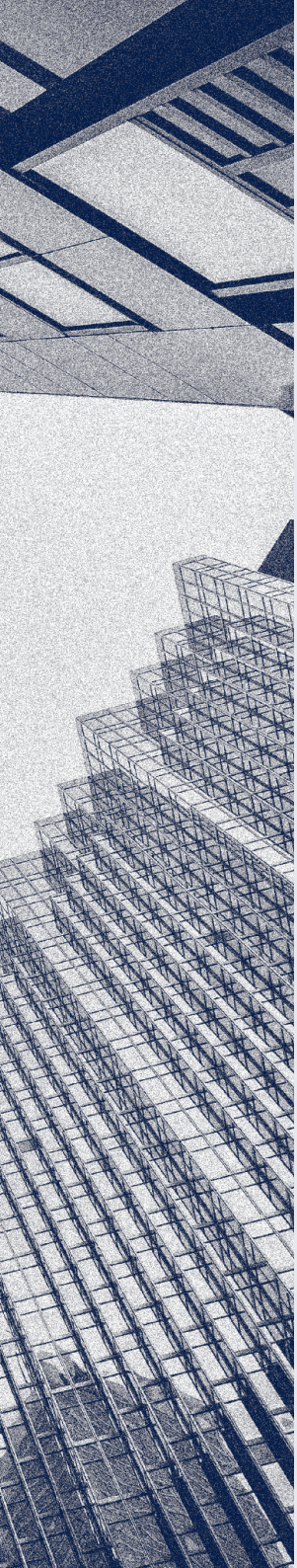
Details

Specific authorities defined

- The Office of the Privacy Commissioner of Canada
- The Commission on Access to Information of Quebec

Specific conditions defined

- A clear explanation of the use of any automated decision system that could significantly impact individuals must be provided under the proposed Consumer Privacy Protection Act.
- Developers of biometric systems used for identification and inference are required to publish a plain-language description of the system under the proposed Artificial Intelligence and Data Act.
- Companies must disclose any processing involving biometric information to the Commission on Access to Information of Quebec.



CANADA

CONTEXT

In 2020, Canada was struck with a biometric mass surveillance scandal: the Royal Canadian Mounted Police (RCMP) and other Canadian police forces were revealed to be clients of the US-based company Clearview AI, which collected billions of images without consent to create a facial recognition database, alongside forces in eighteen European countries.[201]

The Office of the Privacy Commissioner of Canada (OPC) investigation found that Clearview AI had violated federal and provincial privacy laws by scraping images without permission. The provincial authorities issued legally binding orders requiring Clearview to cease offering its services, stop collecting and using images without consent, and delete the collected images and biometric facial arrays of individuals in the provinces.[202] Clearview AI announced in July 2020 that it would stop offering its facial recognition technology in Canada.

The case was also used by the Canadian Privacy Commissioner himself, Daniel Therrien, to emphasise the shortcomings of existing federal privacy laws, pointing out that the Personal Information Protection and Electronic Documents Act (PIPEDA) does not grant powers to the OPC to issue orders nor to impose monetary penalties.[203]

The RCMP later admitted to using other facial recognition tools marketed as software to combat human trafficking and child sexual exploitation.[204] Such use of FRT by the police forces in Canada has raised concerns about privacy, accountability and the need for clear and comprehensive legislation. In a joint statement, Federal, Provincial, and Territorial Privacy Commissioners have emphasised the importance of explicitly defining when

law enforcement can (and cannot) use facial recognition in order to prevent generalised surveillance.[205]

These events led to an extensive study by the House of Commons Standing Committee on Access to Information, Privacy, and Ethics (ETHI). In early October 2022, ETHI released the final report on the use and impact of facial recognition technology: "Facial Recognition Technology and the Growing Power of Artificial Intelligence".[206] The report concludes that "Canada's current legislative framework does not adequately regulate FRT and AI. Without an appropriate framework, FRT and other AI tools could cause irreparable harm to some individuals".

The Committee stressed the need for a robust legislative framework that safeguards privacy rights and civil liberties. Given the absence of such a framework, the Committee proposed a national moratorium on the use of FRT, especially by police services. The report emphasised the importance of granting greater powers to the federal privacy commissioner, including issuing orders and imposing substantial fines similar to those under the EU General Data Protection Regulation. It also highlights the lack of transparency as a significant issue with law enforcement's use of FRT. The public typically obtains information about the use of the technology through media reports, leaked documents and freedom of information requests.

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) released a report in September 2020 on the use of facial recognition at the Canada-US border.[207] It points out that the adoption of facial recognition systems extends surveillance beyond the border, enables repurposing beyond the initial context, and enables automation of other assessment tools. The lack of legal safeguards allows for ad hoc adoption without accountability. The report concludes that Canada's adoption of facial recognition more broadly has lacked transparency and sufficient safeguards.

While the ETHI Committee calls for a moratorium, a collective of 77 privacy, human rights and civil liberties advocates, including the International Civil Liberties Monitoring Group, sent a letter to the Minister of Public Safety in 2020, urging a complete ban on the utilisation of facial recognition surveillance by federal law enforcement and intelligence agencies.[208]

LAW

Canada currently has a patchwork of laws that govern biometrics: the Canadian Charter of Rights and Freedoms,[209] the common law and other laws, including privacy legislation. Current federal privacy laws, the Privacy Act (1985)[210] and the Personal Information Protection and Electronic Documents Act (PIPEDA, 2000)[211] also offer provisions that regulate biometrics, although already several decades old. Experts point out that fragmented legislation at the federal, provincial and territorial levels needs to be replaced with one overarching piece of legislation that comprehensively covers the public, private, non-profit sectors and political parties.

Canada currently lacks a comprehensive legal framework for regulating AI. However, it has implemented the Directive on Automated Decision-Making (ADM Directive),[212] which imposes requirements on the federal government's use of automated decision systems, primarily focusing on risk management. The ADM Directive lacks specific provisions for any kind of biometric surveillance technologies and does not cover AI systems used in the criminal justice system. As such, it allows the federal government to adopt different controversial technologies without complying with the Directive.

Canada's federal privacy regulations are currently undergoing a significant overhaul in the form of the new act called Bill C-27, which may provide an opportunity to fix some of the gaps in the existing legislation.[213] Bill C-27 will introduce three new acts: the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (PIDPTA), and the Artificial Intelligence and Data Act (AIDA).

The Privacy Act and PIPEDA

Canada has two federal privacy laws: the Privacy Act (1985), which governs the federal government's use of personal information, and the Personal Information Protection and Electronic Documents Act (PIPEDA, 2000), which applies to businesses. The Privacy Act applies to services such as pensions, employment insurance, border security and taxation, but it does not apply to political parties.

PIPEDA sets rules for the collection, use and disclosure of personal information by private companies engaged in commercial activities, except in Alberta, British Columbia and Quebec, where similar provincial laws apply.

PIPEDA also applies to federally-regulated companies and their employees' personal information. Provincial privacy laws exist for government agencies, health-related information, employment-related information, and sector-specific laws.[214]

PIPEDA and the Privacy Act do not define biometric data differently than other types of personal data. The Privacy Commissioner of Canada published decisions related to biometric data in multiple cases, including voice authentication in the employment context and collecting fingerprints for taking a Law School test.[215] In those cases, the Privacy Commissioner applied the standard test to evaluate the appropriateness of the purpose expressed for collecting the personal data, asking the following questions:

- is the measure demonstrably necessary to meet a specific need;
- is it likely to be effective in meeting the need;
- is the loss of privacy proportional to the benefit gained; and
- is there a less privacy-invasive way of achieving the same goal?

In 2021, the Office of the Privacy Commissioner of Canada (OPC) updated its guidance to clarify the types of personal information generally considered sensitive under the PIPEDA and added biometric data to that group.[216] Under PIPEDA, private companies must protect sensitive personal information with appropriate safeguarding measures and seek express consent when the information is likely to be considered sensitive.

BILL C-27: CPPA, PIDPTA & AIDA

Bill C-27, also known as the Digital Charter Implementation Act 2022, is the second attempt to overhaul the federal privacy regime. This proposal seeks to establish three new pieces of legislation: the Consumer Privacy Protection Act (CPPA), the Personal Information and Data Protection Tribunal Act (PIDPTA), and the Artificial Intelligence and Data Act (AIDA).

The CPPA and PIDPTA are revised versions of legislation introduced in 2020, which did not pass due to the dissolution of Parliament for the 2021 federal election, while the AIDA is an entirely new legislation. As a result, the Personal Information Protection and Electronic Documents Act (PIPEDA) will be amended to become the Electronic Documents Act,

removing the privacy provisions while retaining the provisions related to electronic documents.

Under the proposed CPPA, private companies would be required to provide a clear explanation of their use of any automated decision system that could significantly impact individuals. That includes systems that make predictions, recommendations or decisions about individuals. Upon request, companies using such systems must also provide individuals with an explanation of how their decisions are made, more specifically, the "type of personal information that was used to make the prediction, recommendation or decision, the source of the information and the reasons or principal factors that led to the prediction, recommendation or decision".[217]

Private companies that violate the provisions of the CPPA can face significant penalties: administrative monetary penalties can be imposed, ranging from up to Can$10 million or 3% of the company's gross global revenue for general violations, and up to Can$25 million or 5% of the company's gross global revenue for certain intentional offences. The Privacy Commissioner of Canada will not directly issue these penalties: the Commissioner will recommend penalties to the Personal Information and Data Protection Tribunal, which will have the authority to impose penalties. Appeals of other orders issued by the Commissioner can also be made to the Tribunal.

The introduction of the AIDA represents one of Bill C-27's most significant changes, which aims to impose new governance and transparency obligations on businesses designing, developing and using artificial intelligence (AI) systems. Under this newly-proposed act, anyone responsible for an AI system must determine if it qualifies as a "high-impact system". If it does, they must implement measures to identify, assess and mitigate potential risks, such as harm or biased outcomes caused by the system. Compliance with these measures must be monitored and documented as well.

The AIDA's approach of categorising AI systems based on their level of risk aligns with the European Union's approach to AI regulation. However, the specific definition of high-risk systems is yet to be established through future regulations. It is also worth pointing out that the EU AI Act explicitly bans specific AI systems that are deemed unacceptably harmful, such as manipulative or exploitative systems and real-time remote biometric identification used by law enforcement — while the current AIDA proposal does not include an outright ban on AI systems with unacceptable risks.

Another key difference is that the scope of the AIDA might be more limited compared to the EU Act. The AIDA's definition of AI systems only covers technological systems that process data autonomously or partly autonomously. In contrast, the EU Act does not necessarily require any degree of autonomy, and includes AI systems developed using specified techniques like machine learning, logic-based approaches and statistical approaches.

Without providing an exhaustive list, the AIDA Companion Document issued by Innovation, Science, and Economic Development Canada (ISED) includes examples of systems that might belong to the high-risk category.[218] Among them are biometric systems used for identification and inference, and systems used to make predictions about people. ISED points out that "such systems have the potential to have significant impacts on mental health and autonomy".

Under the transparency provisions, developers of high-impact systems are required to publish a plain-language description of the system on a publicly-available website. This description should include information about how the system is intended to be used, the types of content it generates, the decisions or predictions it makes, and the mitigation measures in place. In addition, anyone responsible for a high-impact system must promptly notify the Minister if the system causes or is likely to cause material harm.

The proposed Act would introduce significant penalties for violations: administrative fines for breaching governance or transparency requirements can be up to Can$10 million or 3% of gross global revenues. New criminal offences related to AI systems are also proposed, with fines for businesses up to Can$25 million or 5% of gross global revenues. Individuals can face fines of up to Can$100,000 or imprisonment for certain offences. These offences include knowingly using personal information obtained unlawfully, designing or using harmful AI systems, and causing substantial economic loss with fraudulent intent. Notably, these proposed penalties are higher than those in existing legislation, such as Quebec's Bill 64 (see next section) or the EU's General Data Protection Regulation.

The enforcement of AIDA, excluding criminal offences, would be overseen by a newly-established AI and Data Commissioner. Criminal prosecution would be the responsibility of the Public Prosecution Service of Canada (PPSC), with the Minister having the ability to refer cases to the PPSC, but no further involvement in the process. Additionally, external experts

would support the administration and enforcement of AIDA, independent auditors would conduct audits, and an advisory committee would be appointed to assist with enforcement activities.

The proposed timeline for the adoption of AIDA means that any new rules would not enter into force before 2025 at the earliest.

Quebec

In 2001, Québec was the first jurisdiction in Canada to introduce an act to establish a legal framework for information technology (QC IT Act), which includes specific provisions for the use of biometric databases in order to ensure an adequate level of protection.[219] The recent amendment to the QC IT Act, known as QC Bill 64, imposes new requirements related to the reporting of biometric systems used for identification or verification purposes. Companies must disclose any processing involving biometric information, regardless of whether it is stored in a database, to the *Commission d'accès à l'information* (Commission on Access to Information, CAI) — at least 60 days before the biometric database is put into operation. The CAI has powers to set up, manage and order the destruction of such databases if they do not comply or invade privacy. Finally, Bill 64 designates biometric information as sensitive, which means companies should have additional safeguards when processing it.

To mitigate the legal risks associated with processing biometric information, companies must consider the intrusiveness of the technology, the purpose of use, alternative processes, and how biometric information is managed and destroyed. Assessing the level of privacy risk can help establish guidelines and conduct privacy impact assessments (PIAs) to identify and mitigate risks. PIAs will become mandatory from 22 September 2023 under QC Bill 64 when sharing personal information outside of Quebec, creating or acquiring digital systems involving private data, or disclosing personal information without consent for research purposes.

Experts point out that the problem with Quebec's privacy legislation is that it imposes obligations only when biometrics are used to verify identity, arguing that its scope should be expanded for other purposes as well.[220] The Centre for Media, Technology, and Democracy and the Cybersecure Policy Exchange recommended harmonising the Privacy Act and PIPEDA with the federal government's Directive on Automated Decision-Making.[221]

CASE LAW

The Supreme Court of Canada recognised the constitutional right to privacy decades ago, in *R. v Dyment* (1988) 2 S.C.R. 417.[222] The decision highlights that "privacy is at the heart of liberty in a modern state ... [g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state."

In *R. v Spencer* (2014) SCC 43, the Supreme Court of Canada ruled that individuals retain a right to privacy even when in a public space.[223] The Supreme Court pointed out that people often behave differently when they suspect that they are being watched, and this fear of surveillance itself "destroys the sense of relaxation and [behavioural] freedom" that anonymity confers — narrowing the range of autonomous choices available to the actor.

In *Wansink v Telus Communications Inc.* (2007) FCA 21 the Federal Court of Appeal upheld a decision by the Privacy Commissioner of Canada that found that collecting and storing voiceprints of employees for voice recognition technology used to access a company's internal computer network remotely did not violate the privacy of employees.[224] The Federal Court of Appeal found that the purposes for collecting the information were reasonable and that Telus had taken appropriate security measures to protect that information. It also ruled that consent must be obtained from employees, but noted that Telus could not obtain voiceprints without an individual's knowledge and participation. The Court expressed an opinion that voiceprints were not sensitive data.

In *IKO Industries Ltd. v. U.S.W.A.* (2005) the Ontario arbitrator determined that the use of a fingerprint scanning system by an employer was an invasion of employees' privacy and could not be justified.[225] IKO Industries Ltd. (the employer) appealed the arbitrator's ruling, but the Ontario Superior Court of Justice upheld the decision, stating that it was based on a balancing of the employer's and employee's interests. In this case, the invasion of privacy was not deemed to be substantial, but the employer's interest nevertheless did not outweigh it, considering the circumstances of the workplace and available alternatives.

However, in another arbitration case, Agropur, Division Natrel and Teamsters Local Union No. 647 (Slotnick), 2008 CanLii 66624 (ON L.A.), an arbitrator determined that the fingerprint scan was not invasive of privacy.[226] The arbitrator considered relevant biometrics cases decided under labour law, rather than privacy law, and concluded that the scan took less than a minute, did not involve private body parts, and only captured half a fingerprint, which was immediately converted into a series of numbers with no personal information.

CHINA

What type of act regulates processing of biometric data

Data protection law
Yes; the Personal Information Protection Law, 2021.

Bylaws
Yes.

Guidelines
Yes.

Special law on biometric data
Yes, at the level of bylaws.

Law enforcement law
Yes, the national security and counter-terrorism laws.

Criminal Law
Yes, the national security and counter-terrorism laws.

Defining and regulating facial recognition

Data obtained through facial recognition is regulated as sensitive data.

Details

Specific use cases defined
- The Personal Information Protection Law regulates the use of videos captured by cameras in public spaces.

Specific authorities defined
- The Cyberspace Administration of China serves as a supervisory authority with the power to conduct inspections, issue fines, as well as provide opinions and guidance.

Specific conditions defined
- The Personal Information Protection Law establishes rules regarding purpose limitation and recognises the concept of legal basis for processing.
- Transparency requirements are specifically regulated under the Personal Information Protection Law.
- Under prescribed conditions, impact assessment must be prepared.

CHINA

CONTEXT

Mass surveillance in the People's Republic of China is one of the most sophisticated networks of monitoring systems used by a central government on its citizens. China's modern surveillance scheme started in 2003, with the creation of the "Golden Shield Project" that was primarily focussed on internet censorship.[227]

Following the Golden Shield Project, China launched two more surveillance programmes: Safe Cities (2003), which focuses on disaster warnings, traffic management and public security, and SkyNet (2005), the facial recognition programme. According to some reports, "Skynet can scan the entire Chinese population in one second with 99.8 percent accuracy" (allegedly, this number was provided by Chinese state-run media).[228] However, this figure should be taken with a grain of salt given that it has not been independently verified — as well as the fact that given the size of the population of China, such level of accuracy amounts, in fact, to many millions of errors.

However, what is clear is the notable amount of spending on surveillance in China, as its budget far exceeds that of other municipal services, with an estimated 176 million surveillance cameras in operation as of 2017.[229]

Biometric surveillance is mainly used in urban areas in China. By 2010, Beijing alone had accumulated 800,000 surveillance cameras, with the Beijing police boasting in 2015 that the city was 100% covered.[230] In May 2018, facial recognition software alerted concert security that one of the 60,000 concert goers was a suspected fugitive, resulting in the arrest of the 31 year old man within minutes.[231] At some crossroads in Shanghai, jaywalkers must pay a 20 yuan fine and have their pictures shown on a nearby screen for public humiliation.[232]

The extent of facial recognition in China is significant, as Chinese police are reported to have deployed facial-recognition technology in their glasses in early 2018, with Beijing-based LLVision Technology Co. also selling basic versions to countries in Africa and Europe.[233] One can reportedly buy a meal at KFC in Hangzhou using the "Smile to Pay" system with customers' faces linked to their Alipay accounts, or board a bus in Yinchuan simply with a positive facial ID.[234]

These practices are primarily conducted through the government, although corporate surveillance in connection with the Chinese government has been reported to occur. Software companies Megvii and Neurosoft are involved in the harvesting of data from over twenty sectors of the Chinese government and tens of millions of social videos that can detect and identify some basic personal information.[235] Though they deny the accusation, as discussed in the Technology section of this book, the company Megvii collaborated with Huawei to develop a "Uyghur alarm" that can automate the detection of Uyghur faces in video monitoring.[236]

Much of the controversy surrounding FRT in China comes amidst the "Strike Hard against Violent Terrorism" campaign, carried out by the Chinese government in the province of Xinjiang.[237] At police checkpoints, Uyghurs frequently have their DNA collected, eyes scanned and the potential forcing of spyware installed on their phones to track all online activity.[238] These measures come as an asymmetric response to several terrorist attacks in Beijing in 2013-2014, culminating in the detention of roughly one million Uyghurs in various camps, centres and prisons across Xinjiang.[239]Xinjiang is an important case study as it shows how greater biometric surveillance capacity can increase overt repression. Nearly every resident of the region has submitted their biometric data to the authorities with thousands of face-scan and phone-scan checkpoints at jurisdictional boundaries in operation.[240] This comes amidst the worrisome repatriation of Uyghurs from other countries, as since the beginning of the Strike Hard against Violent Terrorism campaign more than 1,300 Uyghurs have been detained, deported or extradited.[241]

Additionally, security services in Xinjiang have even "begun to deploy flocks of smal bird-like surveillance drones to cover areas that CCTV feeds do not track".[242]

China uses various surveillance techniques, such as camera or internet surveillance, to constantly monitor its citizens.[243] Huawei's Safe City product

uses social media monitoring and facial and licence-plate recognition to create "security" in Chinese cities. It has become increasingly widespread and grown in sophistication under the general secretary of the Chinese Communist Party Xi Jinping's administration.[244]

The "Safe City" software had been rolled out across 73 cities in 52 countries by 2019, including Germany, France, Pakistan, Spain and Serbia.[245] In 2019, Serbian authorities moved to deploy 8,000 cameras, with Belgrade city centre being blanketed with facial-recognition surveillance-capable cameras, as we will explore further in the next chapter.[246] Thus, we can see that the biometric advancements happening in China are not occurring in a vacuum.

The party-state's ideological and political imperatives are supported by China's legal system, featuring laws and regulations that govern the creation and use of surveillance technologies by private, state-owned or state-invested firms.[247] Instead of developing a climate that is favourable to protecting the exercise of citizens' rights, China's regulatory system forces businesses to serve as the "surveillance agents of the state".[248] This is, at least in part, because the legal framework in China for surveillance technologies is based on an overly expansive definition of national security, which serves as justification for a broad range of surveillance practices.[249]

LAW

Overview of data protection legislation

Laws that regulate privacy rights and data protection issues have started to emerge in China in the past couple of years, and at least on paper, they do seem to be in line with modern data protection regulations, and are written in legal style as influenced by EU law (the GDPR and its predecessor, the Data Protection Directive from 1995).[250]

Unlike in European legal tradition, privacy is not a constitutionally protected human right in China.[251] The first law that regulates privacy as a legally protected right is a Civil Code,[252] which came into force on 1 January 2021. The right to privacy and personal information are classified as "personality rights", and in case they are violated, the Civil Code provides for legal remedies (from the perspective of torts regulation).[253]

Since November 2021, China also has a Personal Information Protection Law (PIPL), which was adopted in August 2021 and came into force on 1

November the same year.[254] The PIPL is the first law that regulates personal data protection matters in a comprehensive manner. Only a couple of years earlier, in 2016, Chinese legislation got its first legal definition of personal information that is contained in 2016 Cybersecurity Law.[255] In 2021, another important law dealing with data protection matters was issued, called Data Security Law.[256] These three laws together regulate the general personal data protection regime in China.

In addition, there are a number of laws in China that regulate the matters of national security and thus might be relevant for a legal regime pertaining to mass biometric surveillance. These are, in particular: (i) 2015 National Security Law;[257] (ii) 2015 Counter-Terrorism Law;[258] and (iii) 2017 National Intelligence Law.[259] In order to help the government's efforts to maintain national security, these laws regulate general requirements for how private businesses must collaborate and support the government's law enforcement and technology needs.[260]

Certain data protection-related matters are also contained in the sectoral laws (as well as secondary legislation) that regulate personal data processing from the perspective of their main subject of regulation. Such is the case, for example, with the Criminal Law; the E-commerce Law; the Law on Resident Identity Cards; the Law on the Protection of Rights and Interests of Consumers; and the Tourism Law.[261]

Furthermore, the Supreme People's Court and the Supreme People's Procuratorate issue law interpretations, some of which might be relevant for processing biometrics, notably "Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases involving the Processing of Personal Information Using Facial Recognition Technology".[262]

Competent state bodies also issue national standards that are usually not mandatory but are "generally regarded as good-practice guidance by enterprises",[263] whereas the "Information security technology – Personal information (PI) security specification"[264] and "Information Security Technology – Requirements for Security of Face Recognition Data"[265] standards specifically deal with FRT.

Some of these laws regulate very similar or even the same topics, since they were enacted in the timeline where systematic rules, contained mostly in the Civil Code and PIPL, were issued after certain specific legislation (as

will be discussed further in this section). For this reason, the Chinese data protection legal regime is complex, due to overlapping rules on the same matter and unclear distinction of legal regime for public and private actors.

Legal provisions relevant for biometric surveillance

Civil Code

The Civil Code dedicates a whole chapter to "Rights to Privacy and Protection of Personal Information" (Chapter VI). The definition of personal information from Article 1034 explicitly includes "biometric information", but there is no further definition of such biometric information, nor are biometrics included in a "sensitive" data category. The Civil Code contains several general rules (some of which are pretty GDPR-like) around personal information processing, such as:

- **Principles of processing** (Article 1035) — processing must be "in compliance with the principles of lawfulness, justification, and within a necessary limit, and shall not be excessively processed".
- **Conditions for processing** (Article 1035) — processing is allowed if: (i) a person gave consent for processing of their data or processing is otherwise permitted by the law or administrative regulation (therefore, legal acts that are part of secondary legislation, which are lower that the laws, can provide legal basis for processing of personal information); (ii) transparency is secured; (iii) the purpose, method, and scope of the processing are clearly indicated; and (vi) processing does not violate any legal rules.
- **Citizen rights** (Article 1037) — several types of rights are regulated, including right to copy, right to rectification and right to deletion, but in very general terms.
- **Disclosure and data safety** (Article 1038) — there are general rules that limit situations when data sharing is possible, as well as general provisions regulating security measures to prevent data from "being leaked, tampered with, or lost" (including a notification obligation towards competent regulatory authorities and persons affected).

The Civil Code also has a provision (Article 1036) that regulates when an "actor" that processes personal information shall not bear any civil liability for such processing. Two such situations are when there is consent and when data are already public (which is similar to the ''manifestly made public" rule from Article 9 of the GPDR). But the third situation is very widely defined and includes instances when "the actor reasonably performs the other acts to protect the public interest or the lawful rights and interests of the person". Public interest is not defined in the Civil Code, and we can only speculate which government-related surveillance project it could cover. As is always the case with such broadly defined rules, or even legal standards, court practice should provide some clarification and guidance.

Finally, the Civil Code does include general rules concerning the confidentiality obligations of the state, public organs and public officials, but does not regulate sanction for violations of these rules.

Overall, the rules from the Civil Code provide some rights to citizens, which can be enforced in accordance with other domestic laws, but do not provide guidance in terms of state obligations in the context of mass surveillance projects — apart from "principles" provisions, whose relevance remains to be tested in practice.

Personal Information Protection Law

The PIPL is to a large extent inspired by the GDPR text and structure (including with respect to the legal basis for processing, notification and transparency duties, quality of consent, citizens' rights, security measures, cross border transfers, etc.). Unlike the GDPR (and regulations in Kenya and South Africa, for example) it does not exempt any state bodies from applying its provisions. It does, however, have a separate five-article Chapter that regulates "Special Provisions on the Processing of Personal Information by State Organs".

According to these provisions, state bodies must process information in accordance with applicable sectoral laws, but must not "exceed the scope and limits necessary to perform their statutory duties" (Article 34). As will be shown below, this is one of several general principles that may legally affect mass biometric surveillance projects in China, while relevant and concrete legal limitations, duties and restrictions are scarce in legislation reviewed for this book. According to this Chapter of the PIPL, state bodies

also have to fulfil their transparency duties and store data in the Republic of China (with some limited exceptions).

In general, the PIPL has a GDPR approach when it comes to processing biometric data that are regulated within the wider category of "sensitive personal information". However, it does have one provision that specifically regulates use of facial recognition technology in public spaces (although it does not use the phrase "facial recognition" in this particular Article).

Namely, Article 26 of the PIPL reads: "*Image collection and personal identification equipment in public places shall be installed only when it is necessary for the purpose of maintaining public security, and shall be installed in compliance with the relevant provisions of the state and with prominent reminders. The personal images and identification information collected can only be used for the purpose of maintaining public security and, unless the individuals' separate consents are obtained, shall not be used for any other purpose.*"

The first matter worth noting is that this provision does not regulate any data processing that involves facial recognition, but focuses on the installation of equipment and collection of data. It, therefore, does not have anything to say about the processing of images or video that were not collected in public spaces. When it comes to the collection of images in public spaces, the provision contains a three-fold rule: (i) the only permissible purpose for the installation of identification equipment and collection of images is "maintaining public security" (that is not defined in the PIPL) and no other purpose is allowed, aside from the narrow exception when consent is obtained (according to Article 14 of the PIPL, consent must be "voluntary, explicit, and fully informed"); (ii) there must be transparency in the sense that "reminders" should be in place that notify the public about the collection of images and possibility of identification (this notification requirement is emphasised in this Article, in addition to the general "openness and transparency" principle form Article 7); (iii) all other state legislation must be complied with during equipment installation and data collection. Even though it is not explicitly stated in this provision, based on its phrasing we can speculate that only the state can install equipment for facial recognition in public spaces. It can do so only in order to "maintain public security", which is a single but wide enough purpose to include all sorts of state-related initiatives. One could interpret such a broad purpose as covering almost any public authorities' aim, with no guarantees that these public authorities will

not overuse, or even misuse the technology. In practice, this could serve as an "open door" for various mass surveillance state projects.

The PIPL also recognises the notion of automated decision-making in its Article 24, and regulates transparency and fairness rules when this type of processing is in place. Similar to the GDPR, Article 24 of the PIPL regulates a situation when this processing is used to make a decision that may have a significant impact on an individual's rights and interest. If that is the case, the individual has the right to request clarification as well as the right to refuse the decision that is made *only* through automated decision-making.

Moreover, "sensitive personal information" is defined somewhat differently in the PIPL than in the GDPR. Namely, there is an open-ended definition according to which this is "information that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his personal safety or property, including information such as biometrics [...]" (Article 28). Since biometrics are explicitly included as the first type of such information, it is clear that they are covered by this definition, though the PIPL does not further define "biometrics" (same as the Civil Code).

The PIPL does not expand too much on the regulation of sensitive information processing when compared to the Civil Code. According to PIPL provisions, the following rules apply:

- Any processing of sensitive information is allowed "only when there is a specific purpose and when it is of necessity, under the circumstance where strict protective measures are taken" (Article 28).
- Under the general regime, processing of sensitive information must be based on consent, and special transparency rules include the duty to provide information on the impact it has on the individual's rights and interests (Articles 29 and 30).
- Special rules must be developed by entities that process data of minors under 14, with no further guidance on what these special rules should regulate (Article 31).
- Other laws and regulations can regulate processing of special personal information, in which case these provisions shall prevail

over the provision of the PIPL — presumably in line with the general limitation from Article 28.

In addition, according to Article 55 of the PIPL, the "report of the impact assessment on personal information protection" and "the processing record" must be prepared when there is processing of sensitive personal information or automated decisions making. While the minimum content of this report is regulated in Article 56, there are no rules that such a report must be reviewed or approved by some independent authority (which is a standard rule in EU legislation from where this institute of "assessment" is taken from).

Therefore, other than general purpose limitation, necessity and security requirements, there are no other rules in the PIPL which would explicitly limit processing of biometric information on a mass scale by the state, subject to applicable legislation.

Other legislation

The Chinese **Counter-Terrorism Law** regulates to some extent the surveillance powers of the state. Namely, according to Article 27 of this law, local governments at all levels have the obligation to "organise and supervise relevant construction units in allotting and installing public security video image information systems [for] prevention of terrorist attacks, at the key positions of main roads, transportation hubs and public areas of the city as needed". In addition, pursuant to Article 32, competent bodies must establish a public security video information system and ensure its regular operation. Video or images gathered via such systems data must be kept for at least 90 days. The Counter-Terrorism Law does not spell out that this video equipment cannot be used for any purpose other than anti-terrorism activities, although such a rule could be indirectly implied from the purpose limitation principle regulated in Article 28 of the PIPL.

The **Cybersecurity Law** and **Data Security Law** do not have anything specific to say about processing of biometrics or use of face recognition technology. As its name suggests, the Cybersecurity Law deals with the issues of cybersecurity and it applies to "the construction, operation, maintenance and use of networks as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China".[266] Also, as it was issued in 2016, it contained many data protection requirements that were restated in the Civil Code in 2021.[267] The Data Security Law,

on the other hand, "primarily focuses on protecting overall national data security",[268] i.e. it applies to the processing of any, not just personal, data and contains "high-level data management and protection methodologies and rules",[269] for any private or public actors who process data.

In accordance with the Cybersecurity Law, the competent bodies issued the above-mentioned standard called the **Information security technology — Personal Information (PI) Security Specification** (PI Security Specification) in March 2020. This standard regulates certain security requirements that are dedicated specifically to biometric data and facial recognition. The wording of the whole PI Security Specification indicates that it is primarily directed to commercial activities, as this is the context in which the document is written. Article 1 states that it applies to "processing activities carried out by all kinds of organisations" but that it "can also be used by competent authorities". Therefore, the PI Security Specification itself does not aim to regulate the use of FRT by public bodies, although they are "encouraged" to take it into account when deploying such technology.[270]

It might be worth noting, also, that the PI Security Specification was issued one year prior to the PIPL enactment, and regulates some matters that were later covered by the PIPL (e.g. consent and transparency requirements). In case of any discrepancies or doubts as to how certain rules should be interpreted, the provisions of the PIPL should prevail in line with the general interpretation principle *lex posterior derogat legi priori*.

One issue that is not regulated in the PIPL, but is regulated in detail in the PI Security Specification, is retention of biometric data. According to Article 6.3, controllers are not, in principle, allowed to store the "original personal biometric information (such as specimen and images)", subject to some limited exceptions, which include storage on "the terminal that collects such information", until the identification and authentication functions are completed, and after that, original data must be deleted.

Another standard dedicated to facial recognition is the **Information Security Technology — Requirements for Security of Face Recognition Data** (Face Recognition Standard) adopted in April 2022 (although only the 2021 consultation draft is publicly available).[271] Unlike the PI Security Specification, this standard does not make an explicit difference between public and private data controllers. However, in its Article 3.5 (which is the Face Recognition Standard definition of "data controller") it does refer specifically to the definition of "organisation" from

the PI Security Specification in order to determine the entities to which the Face Recognition Standard is applicable. For this reason, it seems that (much like the PI Security Specification) this standard is aimed at private companies' processing activities and not the face recognition practices of state authorities.

The Face Recognition Standard regulates, amongst other matters: (i) the requirement for consent that data controllers must secure if they intend to use face recognition for identification and verification purposes; (ii) rules regarding sharing, transfer and disclosure of facial recognition data; (iii) requirements on the deletion of such data; and (ii) the transparency and security-related duties of data controllers. This standard explicitly prohibits "assessments or predictions of data subjects' work performance, economic status, health status, preferences, or interests" (Article 5).

In addition to these standards, private companies that use facial recognition must also act in accordance with the document titled "**Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases involving the Processing of Personal Information Using Facial Recognition Technology**", which was issued by the Supreme People's Court in July 2021 (Judicial Interpretation). Here, the court summarised case practice from the private sector and provided guidance on several matters from the civil law perspective, such as conditions for valid consent and procedural issues in tort-related cases (e.g. burden of proof, joint and several liabilities, conditions for injunctions and damages).[272]

The Judicial Interpretation was issued before the PIPL came into force and is, therefore, based only on the interpretation of the Civil Code, and does not take into account PIPL provisions. Although Judicial Interpretation does not deal directly with the use of FRT by public authorities, they do have something to say about its use in public spaces. Namely, according to Judicial Interpretation, use of facial recognition technology is prohibited in public places like hotels, shopping malls, banks, airports, sports stadiums and entertainment venues (probably, inter alia, because for practical reasons it cannot be based on consent). This prohibition could be read to mean that any collection of facial recognition data in public spaces can be based only on applicable laws that would regulate such processing — which would be in line with provisions of the PIPL that was adopted one month later.

National authority

According to the PIPL, the Cyberspace Administration of China is an authority in charge of the overall implementation of the law, with the mandate to issue standards and guidance on several matters, including face recognition and artificial intelligence. However, according to information available for this book, there is no guidance when it comes to the collection and processing of biometric data by the state for private purposes, or the use of surveillance tools in public spaces.

CASE LAW

So far, there have been a couple of judgements dealing specifically with the use of facial recognition technology by private entities, but no judgements in cases that would involve state authorities.

The first of this kind was a case involving a law professor who sued Hangzhou Safari Park.[273] The plaintiff bought an annual pass for the park in 2019. At the time, fingerprints were used as a park entry verification method (interestingly, the fact that fingerprints are also biometric data was not problematised by the plaintiff), which the plaintiff provided to the park along with his photo. Later in the same year, the park switched to facial recognition verification. When the plaintiff was asked to register for this type of verification, he refused and sued for breach of contract.[274] The first instance court made a decision in 2020 in favour of the plaintiff on the grounds that the plaintiff did not (and did not have to) consent to use of facial recognition. In line with this reasoning, the court ordered the park to delete the plaintiff's photo, but did not rule that deletion of the plaintiff's other data was mandatory for the park.[275] The plaintiff appealed, also in the hope that the court would issue a more general decision, including guidance applicable to similar cases of facial recognition use, and not just on the merits of this specific case.[276]

The second instance decision was issued in April 2022, and was again only a partial success for the plaintiff. Here, the court upheld the first instance decision, but also ruled on the deletion of fingerprint data — because they were no longer necessary for any purpose (while their initial collection was justified, as it was based on the plaintiff's consent).[277] The court did not, however, have anything to say on whether the park was generally allowed to keep biometric data of all its other customers, or if the park's

"rules of fingerprint and face recognition as the only way to enter the park were invalid".[278] We can only wonder if any of these judgements would be different after the PIPL came into force.

A similar decision was made in a case involving an apartment complex which used FRT as the only means of entry verification. One of the residents sued, and the court "ordered the property management company to delete the facial recognition data, provide alternative access methods and pay compensation".[279] Such a decision was based, inter alia, on the rules and guidelines outlined by the Supreme People's Court in the Judicial Interpretation, which specifically address this scenario.[280] Namely, the Judicial Interpretation makes it particularly clear that a property management business cannot insist that face recognition be used as the exclusive method of identification for property owners entering or leaving their residences.[281]

In recent years across many African countries, there have been numerous initiatives and projects, such as those related to smart cities or reforms of national ID systems, which involve extensive use of technologies that process biometric data.[282] There are some speculations about Chinese influence when it comes to the technology used, as the governments of southern African countries opted to cooperate with Chinese companies when procuring facial recognition technology.[283] In terms of laws and regulations, African countries seem inclined to follow the EU legal tradition, by foregrounding the sensitivity of biometric data and the need to regulate its use.[284]

EUROPEAN UNION

What type of act regulates processing of biometric data

National constitution
Yes. The European Convention on Human Rights, 1950; EU Charter of Fundamental Rights, 2000.

Data protection law
Yes, the General Data Protection Regulation.

Bylaws
Yes.

Guidelines
Yes.

AI Regulation
Yes, the AI Act, currently in the "trilogue" negotiation phase.

Law enforcement regulation
Yes. The Law Enforcement Directive.

Local level legislation
Yes, the member-states national legislation.

Defining and regulating facial recognition

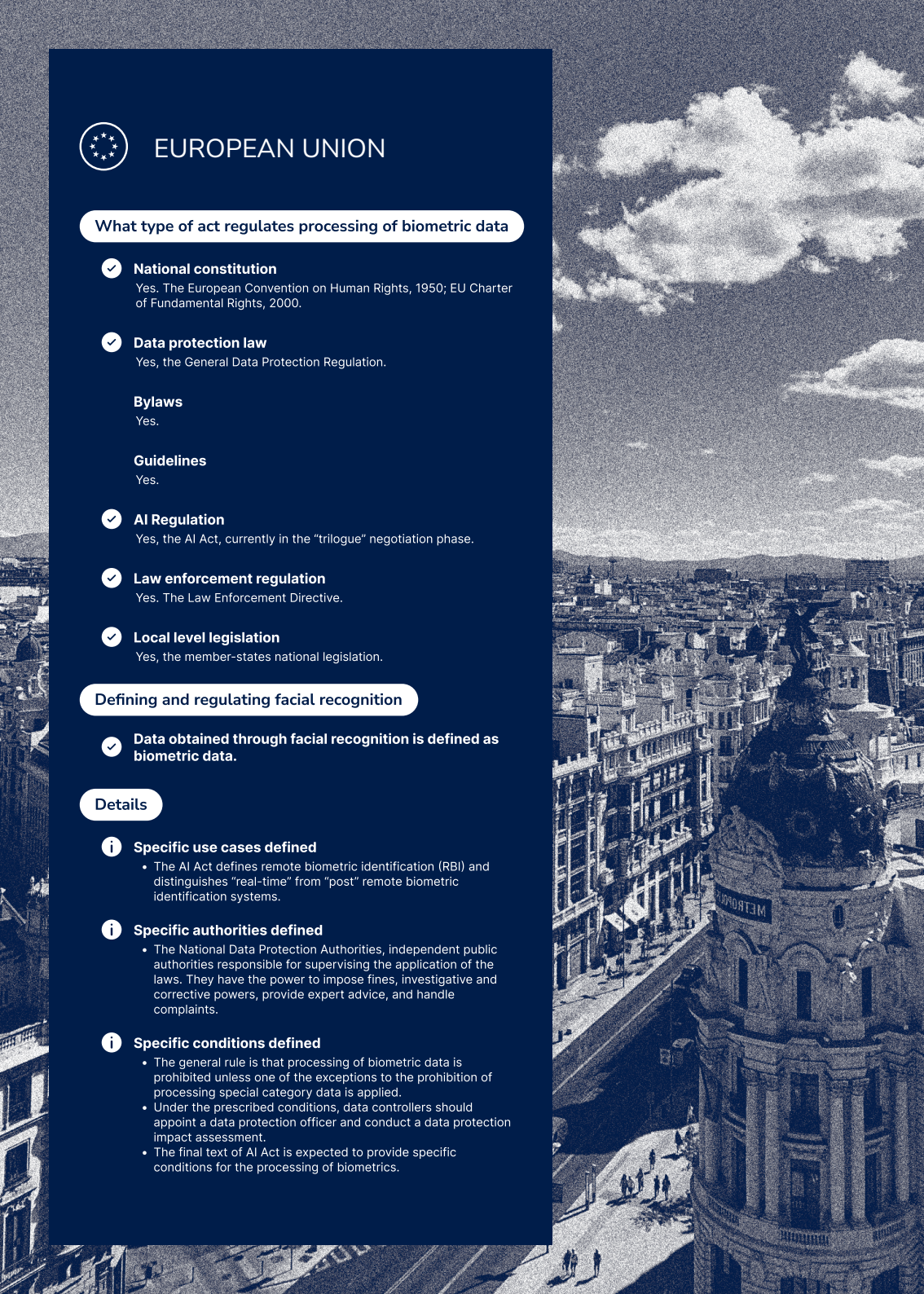
Data obtained through facial recognition is defined as biometric data.

Details

Specific use cases defined
- The AI Act defines remote biometric identification (RBI) and distinguishes "real-time" from "post" remote biometric identification systems.

Specific authorities defined
- The National Data Protection Authorities, independent public authorities responsible for supervising the application of the laws. They have the power to impose fines, investigative and corrective powers, provide expert advice, and handle complaints.

Specific conditions defined
- The general rule is that processing of biometric data is prohibited unless one of the exceptions to the prohibition of processing special category data is applied.
- Under the prescribed conditions, data controllers should appoint a data protection officer and conduct a data protection impact assessment.
- The final text of AI Act is expected to provide specific conditions for the processing of biometrics.



EUROPEAN UNION

CONTEXT

Private and public actors in the European Union are increasingly deploying "smart surveillance" solutions, including Remote Biometric Identification (RBI) technologies,[285] which have been linked to mass surveillance practices.[286] While the current deployments of RBI technologies within the EU are still primarily experimental and localised, there is a worrying progress in two areas: first, the current creation and upgrading of biometric databases used in civil and criminal registries, which underpin both live and retrospective systems; second, the repeated piloting of live systems connected to remote facial and biometric information search and recognition algorithms.

Biometrics have been a crucial element in the border management policies of the EU since they are implemented in visas, passports and identity cards. Today, eu-LISA, the agency responsible for the EU's border and migration systems, manages information systems containing more than 53 million pieces of biometric data.[287] These systems are the VIS, the SIS I and II, Eurodac, the ECRIS, the ETIAS and the EES[288]. Eu-LISA also operates the Automated Fingerprint Identification System (AFIS), which is expected to include facial recognition in the future.[289]

The European Commission has proposed updating the Regulation on automated data exchange for police cooperation — the proposal known as "Prüm II" — aiming to enhance the data-sharing network among Member States. The proposed expansion covers the inclusion of facial images and, optionally, "police records". However, concerns have been raised

regarding potential state overreach and mass surveillance, as it may treat a significant portion of the population as potential criminals and pose risks to privacy and data protection.[290] The proposal also employs the principle of free movement of people to justify heightened policing and surveillance measures.

The legal rules for conducting biometric surveillance in public areas are outlined in the European Union's secondary legislation on data protection, including the General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive (LED). When using biometric data, these regulations require careful consideration of how to protect fundamental rights. The GDPR and LED have been important in setting generally high standards for the protection of personal data in the EU. But they have not always gone far enough. Scholars and activists have argued that the GDPR and the LED are not written precisely enough, leading to potential loopholes, and contain "state friendly exceptions and rules and little or no substantive hurdles to address concrete surveillance technologies".[291]

The draft Regulation laying down harmonised rules on Artificial Intelligence (the Artificial Intelligence Act), which was proposed in 2021, is expected to have a significant impact on the use of biometric identification systems once it is passed.[292] One of the most controversial parts of the proposal is whether it should enforce a complete prohibition on utilising facial recognition (or other forms of remote biometric identification) in public spaces, and if so, which parties should be subject to it: law enforcement agencies only, or all actors, including public agencies and private entities?

In October 2022, the European Parliament passed a non-binding resolution calling for a moratorium (time-limited ban) on police use of facial recognition technology in public places, predictive policing, biometric mass surveillance practices, and a ban on the use of private facial recognition databases.[293] In this context, many international organisations and institutions are calling for bans on various biometric surveillance practices, particularly on facial recognition in publicly accessible places. They include the United Nations,[294] the European Parliament,[295] the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS),[296] as well as more than 170 non-governmental organisations (NGOs).[297]

The most notable civil society initiative in Europe urging a ban on the use of biometric systems which amount to mass surveillance has been the "Reclaim

Your Face" campaign.[298] More than 260,000 individuals have supported the campaign led by a large coalition of civil society organisations, which is considered to have influenced developments in the process of adopting the EU AI Act.

Regarding EU Member States' attitudes towards biometric technologies, we see different approaches. Italy has led the way by becoming the first country in Europe to introduce a moratorium on public facial recognition.[299] Meanwhile, the German coalition government has called for a ban on these practices across the entire EU.[300] In Portugal, a proposed law would have legalised some biometric mass surveillance practices — but has since been dropped.[301]

On the other hand, French legislators have been intensively discussing the implementation of a legal framework that would enable the deployment of two different facial recognition technologies purportedly to increase the safety of major public events, with a particular focus on the Paris 2024 Olympic and Paralympic Games. After a strong pushback from the public, especially from European civil society groups, the French Government eventually rejected using facial recognition during the Paris Games.[302]

However, the French Parliament has recently approved an Olympic and Paralympic Games law which would allow the automated monitoring of public spaces for "suspicious behaviour". Live video footage captured by drones and thousands of CCTV cameras will be analysed, purportedly to identify abandoned bags and monitor crowd behaviour, and also to report any "abnormal" behaviour.

The exact meaning of "abnormalities" remains undefined in the text and is subject to future government decrees. When asked by Members of Parliament to provide other examples, the government was evasive in its response. The Greens/EFA group in the European Parliament calls this "the first introduction of the biometric mass surveillance of public spaces in Europe".[303] The move was also condemned by 41 Members of the European Parliament, representing five of the seven pan-European political groups.[304] And in a further blow, the German coalition government failed to keep its coalition commitment to ban biometric mass surveillance when faced with the opposition of other EU Member States.[305]

LAW

In 1950, the European Convention on Human Rights (ECHR) was signed by all 47 Member States of the Council of Europe, including the UK, to establish clear obligations for states to protect and respect human rights and to create a mechanism for enforcing these rights by overseeing their implementation. The European Court of Human Rights (ECtHR) is responsible for interpreting the ECHR. The EU Charter of Fundamental Rights (Charter) provides equivalent protection to the ECHR at the level of the European Union in terms of the meaning and extent of the rights it safeguards. It is interpreted by the Court of Justice of the EU (CJEU).

Article 7 of the EU Charter and Article 8 of the ECHR guarantee each individual the right to respect for his or her private and family life, home and communications. The Charter enshrines an individual right to the protection of personal data in Article 8.

The legal framework covering biometric technologies can be found in the EU secondary legislation that regulates data protection. The principles of personal data protection are clarified in the General Data Protection Regulation (GDPR),[306] which is applicable in all situations where personal data is being processed, with the exception of cases involving law enforcement activities, when the Data Protection Law Enforcement Directive (LED)[307] applies instead. As a Regulation, the GDPR is directly applicable in all EU Member States, whereas the LED has to be transposed into law in each Member State.

In April 2021, the European Commission — the institution responsible for proposing new EU laws — published its proposal for the Artificial Intelligence Act (EU AI Act) to create a harmonised legal framework regarding the use of AI-based systems across the bloc.[308] The initial proposal includes restrictions on the use of remote biometric identification (RBI) systems for law enforcement purposes.

GDPR and LED

Both the GDPR and the LED define biometric data the same way: "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial

images or dactyloscopic data."[309] We can distinguish two categories of information recognised as biometric data:

- "physical/physiological characteristics" focused on bodily characteristics such as fingerprint image analysis, iris recognition, face recognition, ear shape recognition, and so forth; and
- "behavioural characteristics" like hand-written signature verification, keystroke analysis, or gait (walking style) analysis.[310]

The GDPR and the LED also include biometric data when processed for the purpose of uniquely identifying a person in the special category of personal data,[311] also known as "sensitive data" — which are granted a higher level of protection. It is important to note that biometric data are in that category on the basis of their inherent sensitivity, without having to reveal other sensitive information regarding a person (such as health data, racial origin or sexual orientation) in order to be considered sensitive.

However, there is a particular difference between the approach of the GDPR and the LED to the processing of those special categories. The GDPR prohibits this processing (Article 9) but sets ten exceptions to the rule, including the explicit consent of the data subject, processing necessary to protect the data subject's vital interests, and processing necessary for establishing, exercising or defending legal claims. It also allows Member States to introduce additional conditions regarding the processing of biometric data in their national legislation, in particular to allow for imposing stricter rules on their use (Article 9(4)).

The LED, in contrast, allows the processing of special categories "where strictly necessary" (Article 10), with the appropriate safeguards, and only for three purposes: where authorised by Union or Member State law; to protect the vital interests of a person; or where such processing relates to data which are manifestly made public by the data subject. As such, the LED differs from the GDPR in that it does not start with the presumption of a prohibition.

Automated decision-making and profiling, meaning the use of personal data by automated systems to make a decision or an inference, are common practices in the EU alongside the processing of biometric data. For example, data protection authorities in France, Sweden and Bulgaria have banned the use of automated facial recognition systems in schools for attendance checks and access permission on school grounds.[312] The GDPR and LED define profiling as automated processing to evaluate an individual's personal aspects.

Regarding automated decision-making, the LED prohibits it unless authorised by EU or Member State law (Article 11), which has to provide safeguards for the rights and freedoms of the data subject — with a particular emphasis on the right to obtain human intervention. Article 11(3) of the LED provides an unconditional prohibition against conducting profiling that has a discriminatory effect on individuals based on their sensitive data (including biometric data) under EU law.

The GDPR gives data subjects "the right not to be subject to a decision based *solely* on automated processing", including *profiling* (Article 22(1)). This means that partially automated decisions are not covered by this right, which is often referred to as the "human-in-the-loop" principle. However, there are also three exceptions where this right shall not apply, including entering into a contract, on the basis of law, or with consent.

At the same time, Article 22(4) prohibits automatic decision-making based on special categories of personal data (such as data about gender or ethnicity, or biometric data) on the basis of those exceptions, unless the data subject gives explicit consent or processing is necessary for reasons of substantial public interest. As such, the GDPR does not prohibit automated decision-making and profiling, but rather sets conditions for its use, particularly with regard to sensitive category data. The Regulation also insists on transparency regarding automatic personal data processing: the data subject needs to be informed about the logic and consequences of such processing.

Additional checks are necessary for "systematic monitoring": the GDPR requires a data protection impact assessment (DPIA) in the case of "systematic monitoring of publicly accessible areas on a large scale" (Article 35(3)(c)), and establishes an obligation to designate a data protection officer if the processing "by its nature entails regular and systematic monitoring of data subjects on a large scale". This is of key relevance to the question of biometric surveillance because this definition includes the use of

biometric technologies, such as facial recognition, when monitoring and tracking individuals in public spaces. DPIAs are also required in the case of automated profiling (Article 35(3)(a)) and when processing special category data (Article 35(3)(b)).

The GDPR and LED also established Data Protection Authorities (DPAs), independent public authorities that supervise the application of these laws. DPAs have investigative and corrective powers, provide expert advice on data protection matters, and handle complaints related to violations of the GDPR and relevant national laws, including those within the scope of the LED.

EU AI Act

The proposal for the EU AI Act sets different rules based on three categories of risks that AI systems may create: 1) an unacceptable risk — the use of an AI system is prohibited; 2) a high risk — such an AI system is subject to additional obligations and assessments; 3) low or minimal risk — no additional restrictions, with the exception for limited transparency requirements in limited cases. The impact assessment shows that the majority of systems on the market would fall into the third category.

The Act defines a remote biometric identification (RBI) system in Article 3(36) as "an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified". It also draws a distinction between "real-time" and "post" remote biometric identification systems: only the use of real-time systems in publicly accessible spaces for the purpose of law enforcement is put on the list of prohibited AI practices in the European Commission's draft proposal.

It is important to note that this already narrow proposed RBI prohibition also has three exceptions:

- targeted search for specific potential victims of crime, including missing children;
- prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or a terrorist attack; or

» if related to any criminal offence for which a European Arrest Warrant can be issued, in case it is punishable by a custodial sentence or a detention order "for a maximum period of at least three years" (meaning that the upper threshold for the sentence is from three years to life, a criteria which is designed to ensure only relatively serious crimes are included).

The European Data Protection Supervisor (EDPS), the European Data Protection Board (EDPB) and many civil society groups have criticised these exceptions for being too broad, with European Digital Rights (EDRi) calling them a "'blueprint' for how to conduct biometric mass surveillance practices" rather than a meaningful ban.[313]

Under Article 5, when using "real-time" remote biometric identification systems for any of the three exceptions, the Act insists that "the nature of the situation giving rise to the possible use" and "the consequences of the use of the system for the rights and freedoms of all persons concerned" must be taken into account. Each use within the exceptions needs to be a subject of a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State where the use is to take place — except in a "duly justified situation of urgency". The Act allows Member States to lay down detailed rules for using these systems in their national laws.

The use of "post" (retrospective) remote biometric identification systems for law enforcement purposes is listed as a high-risk AI system (Annex III), which means that its developers have a set of special obligations listed in Chapter 3 of the Act. These include human oversight, "sufficient transparency", quality management systems, and undergoing a conformity assessment. Regarding the latter, while other high-risk AI systems need to go through internal control checks, post RBI systems must be subjected to third-party conformity assessment.

In their opinions on the proposal, the EDPB and the EDPS, the EU's top data protection authorities, alongside numerous civil society organisations, voiced their concerns regarding how the proposed AI Act regulates biometric identification in publicly accessible spaces. In their joint opinion, the EDPB and EDPS called for "a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other

biometric or behavioural signals, in any context", which is significantly more restrictive than the draft AI Act's approach.[314]

In December 2022, the Council of the EU agreed on its general approach (the position of the Council for future negotiations with the Parliament), declaring an even more permissive incline to RBI than the initial draft. The text of its approach further clarified the objectives where it would be considered that such use is strictly necessary for law enforcement purposes.[315] However, In May 2023, the Internal Markets and Civil Liberties committees of the European Parliament, the two working groups in charge of the Parliament's position, voted in favour of banning AI systems used for biometric surveillance, emotion recognition, and predictive policing.[316] MEPs made significant amendments to the list of banned uses of AI systems, which according to their provisional position includes:

- "real-time" remote biometric identification systems in publicly accessible spaces;
- "post" (retrospective) remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorisation;
- biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);
- predictive policing systems (based on profiling, location, or past criminal behaviour);
- emotion recognition systems in law enforcement, border management, workplace, and educational institutions; and
- indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases.

Another notable point is that the Parliament's draft text includes a new definition for biometrics-based data: "Biometrics-based data are additional data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person, such as facial expressions, movements, pulse frequency, voice, key strikes or gait, which may or may not allow or confirm the unique identification of a natural person."

This definition aims to ensure that even where the threshold of unique identification may not be met, the data will still be afforded the same protections as uniquely-identifying biometric data. This includes, for example, the processing of information about hair colour, which typically has not been considered uniquely-identifying biometric data, or emotion recognition, which some suppliers have tried to argue does not constitute personal data. However, distinction is increasingly blurred as technological advances allow an increasingly wide variety of data to be used for the purpose of uniquely identifying a person.

In June 2023, the European Parliament plenary voted in favour of these protections in their official stance on the Artificial Intelligence Act.[317] Following the vote, trilogue negotiations between the European Parliament, Commission and Member States commenced in order to finalise the text. The negotiations are anticipated to be completed by the end of the year, with the goal of passing the law before the European Parliament elections in June 2024.

Civil society has called this vote "a massive win for our fundamental rights" from the perspective of banning biometric mass surveillance, while pointing out that the proposal is still not adequately safeguarding the rights of migrants from discriminatory surveillance practices — since there are no measures addressing AI-enabled illegal pushbacks and discriminatory profiling at the EU border — and contains other residual issues too.[318]

CASE LAW

The obligations from the European Convention on Human Rights (ECHR) are enforced by national judges in all states, parties under the supervision of the European Court of Human Rights (ECtHR) as a last resort. The rulings of ECtHR are binding without the possibility of appeal. The ECtHR has asserted that it "determines issues on public-policy grounds in the common interest, thereby [...] extending human rights jurisprudence throughout the community of [European] Convention States".[319]

The jurisdiction of the Court of Justice of the European Union (CJEU) is limited to acts implementing EU law. Despite this, the CJEU considers both the Charter and the European Convention on Human Rights (ECHR) in its decisions, since the Charter offers the same level of protection for rights that are included in both legal instruments.

Based on the case law of both the ECtHR and the CJEU, as this section will explore, the automated analysis of biometric data amounts to an interference with the fundamental right to privacy and personal data protection. Such an interference therefore has to meet specific fundamental rights requirements in order to be lawful. According to Article 51 of the Charter, any interference with a fundamental right must be necessary, proportionate and duly safeguarded. It cannot infringe upon what is often referred to as the essential core of the right.[320]

While the decisions of national Data Protection Authorities (DPAs) do not hold the same legal weight as judgments made by courts, they can still significantly impact how the GDPR and LED are interpreted and enforced. When a DPA makes a decision on a particular case, it provides guidance on how the law should be interpreted in similar cases in the future. DPAs also have the power to impose fines of up to 4% of a company's global turnover.

ECtHR and CJEU

In the landmark case of *S. and Marper v. the United Kingdom* (2008) the European Court of Human Rights ruled that the generalised and indiscriminate collection and retention of biometric data (DNA samples) from individuals who have not been convicted of a crime violates their right to privacy under Article 8 of the European Convention on Human Rights.[321] The case required the UK government to revise its policy on the retention of DNA samples, and the ruling is applicable to all states parties to the ECHR. In this ruling, the ECtHR also explained that such data have the potential to reveal sensitive personal data, like ethnic origin, which can make people vulnerable to stigmatisation and discrimination.

The ECtHR reiterated this stance in the case of *Gaughran v. The United Kingdom* (2020) and also pointed out for the first time that the taking and retention of custody photographs amounts to an interference with Article 8.[322] This development can be connected to technological advancements, which allowed the application of extensive facial mapping and recognition to such photographs.

In *Uzun v. Germany* (2010) the ECtHR stated that visual or audio surveillance is more intrusive to a person's right to respect for private life than location data because "they disclose more information on a person's conduct, opinions or feelings".[323]

The Court of Justice of the European Union (CJEU) concluded in La Quadrature du Net and others (C-511/18, C-512/18 and C-520/18) (2020) that the automated analysis of traffic and location data was contrary to the right to protection of personal data, granted by Article 8 of the EU Charter.[324] The concept of "strict" proportionality was to be applied for such processing, allowed only if interference was necessary to respond to a severe threat to national security. The CJEU also emphasised that any decision to impose an order for retention of such data must be subject to effective review by either the Court or an independent administrative body with binding authority.

It also recognised that requiring electronic communication service providers to retain traffic data through national legislation not only violated privacy and personal data protection but also clashed with the freedom of expression principle in Article 11 of the EU Charter. Consequently, the CJEU concluded that the automated analysis of traffic and location data would likely discourage individuals from exercising their freedom of expression: "Such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistleblowers whose actions are protected by Directive (EU) 2019/1937."

Likewise, the deployment and use of biometric surveillance in public spaces have similar, if not more severe consequences. It eliminates anonymity, restricts freedom of expression, and deters individuals from participating in public activities.[325] Journalists, activists and political opponents may engage in self-censorship due to the fear of being constantly monitored.

Data protection authorities

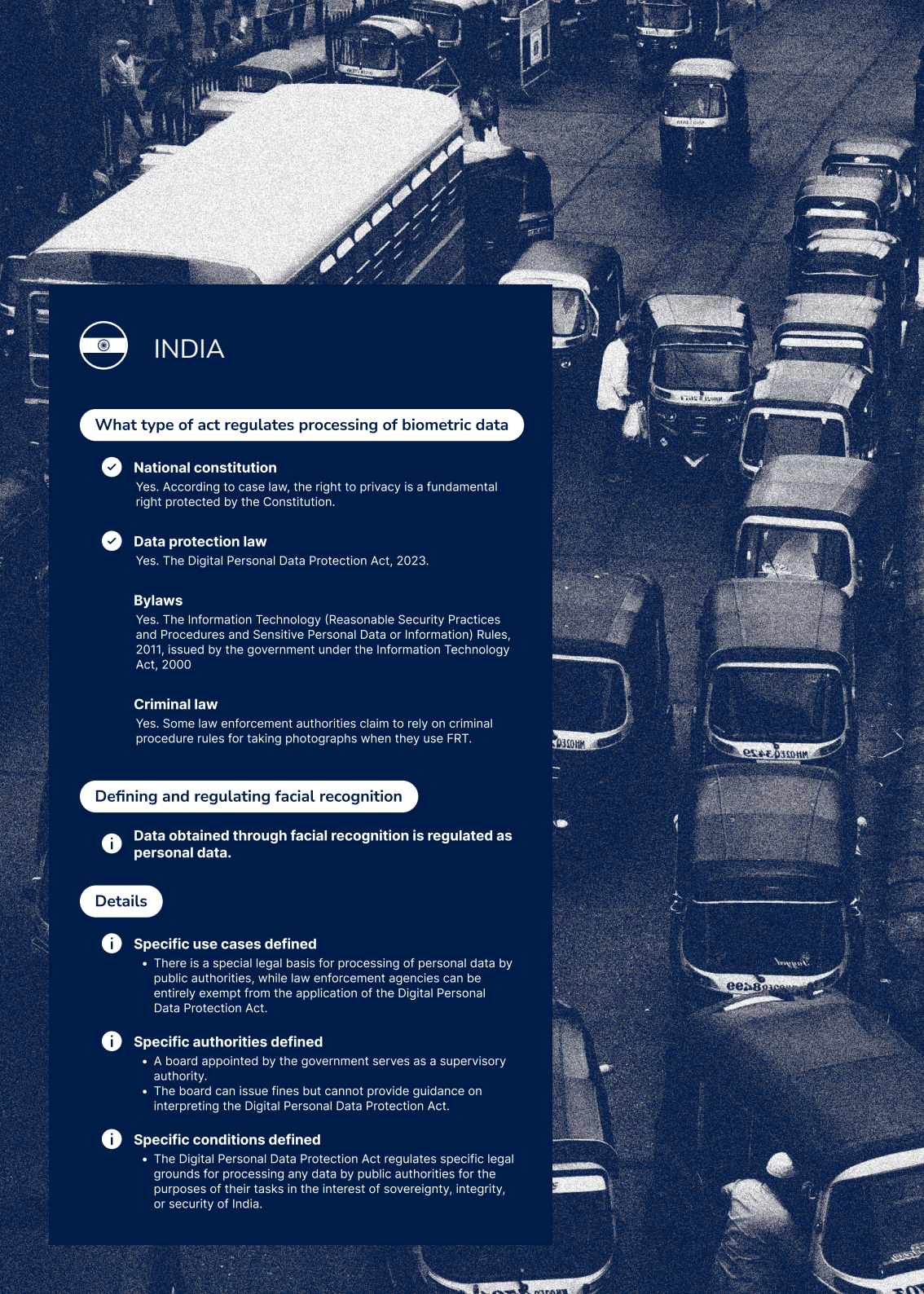
The first GDPR fine ever issued by the Swedish DPA, the Integritetsskyddsmyndigheten (IMY), was for a sum of approximately 20,000 euros levied against a school for using facial recognition technology to monitor students' attendance. The IMY concluded that the school processed sensitive biometric data without a valid legal basis, in violation of the GDPR: they based the processing on consent, which was invalid since there is a clear imbalance between the students as data subjects, and the school as the controller. The school also would have needed to produce an adequate DPIA for the processing, which it did not do.[326] French, Polish and UK DPAs have also ruled against the processing of student's biometric data for similar reasons, with the French CNIL's decision being upheld in

a subsequent court case brought by civil society group La Quadrature du Net.[327]

In a second example, and as briefly discussed in the preceding section, the IMY found that the Swedish Police unlawfully used the facial recognition app Clearview AI — the first time that a DPA targeted the end-user (the police) rather than the provider. The IMY concluded that the police failed to implement sufficient organisational measures, did not conduct a DPIA, and let unauthorised employees use the application. The police were fined SEK 2,500,000 (approximately EUR 250,000) for this breach of the LED.[328]

In a third example, the Italian DPA — the Garante Privacy — rejected the Italian government's attempt to introduce live facial recognition (a system known as "SARI"), explaining that this would amount to "mass surveillance".[329] However, the Garante Privacy permitted a version of the system to be used retrospectively, which was criticised by several civil society groups for drawing an arbitrary technical distinction between practices that are equally harmful. These examples represent only a handful among numerous DPA cases across the EU that relate to facial recognition or other forms of biometric processing.[330]

When considering the case law of the ECtHR and CJEU, as well as the decisions of data protection authorities, it is evident that the EU takes a generally restrictive approach to the processing of biometric data, driven by the aim of safeguarding particular fundamental rights to data protection, privacy and associated rights of non-discrimination.



INDIA

What type of act regulates processing of biometric data

National constitution
Yes. According to case law, the right to privacy is a fundamental right protected by the Constitution.

Data protection law
Yes. The Digital Personal Data Protection Act, 2023.

Bylaws
Yes. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued by the government under the Information Technology Act, 2000

Criminal law
Yes. Some law enforcement authorities claim to rely on criminal procedure rules for taking photographs when they use FRT.

Defining and regulating facial recognition

Data obtained through facial recognition is regulated as personal data.

Details

Specific use cases defined
- There is a special legal basis for processing of personal data by public authorities, while law enforcement agencies can be entirely exempt from the application of the Digital Personal Data Protection Act.

Specific authorities defined
- A board appointed by the government serves as a supervisory authority.
- The board can issue fines but cannot provide guidance on interpreting the Digital Personal Data Protection Act.

Specific conditions defined
- The Digital Personal Data Protection Act regulates specific legal grounds for processing any data by public authorities for the purposes of their tasks in the interest of sovereignty, integrity, or security of India.

INDIA

CONTEXT

The use of facial recognition systems is very common in India, including for law enforcement purposes.[331] The Internet Freedom Foundation (IFF) runs Project Panoptic, which tracks and maps out various facial recognition projects in the country.[332] At the time of writing, the project counted 126 systems installed across the whole of India. However, not all areas in the country are equally subjected to these biometric mass surveillance systems.

The southern Indian state of Telangana seems to be the leading state when it comes to public deployments of facial recognition. The capital, Hyderabad, is sometimes called the "most surveilled city in the world", where it is estimated that the state has more than 600,000 cameras installed,[333] as well as a "command and control centre".[334] The Associated Press has accessed the centre and reports it as a tall tower in which police officers have access to "24-hour, real-time CCTV and cell phone tower data that geolocates reported crimes" and uses facial recognition to search for potential criminals in a vicinity of a crime scene. In addition, the officers have access via phones to an app named TSCOP that has mobile facial recognition scanning capabilities.[335] According to reports, this app is used to take photographs and match them with a police database,[336] which was used during the COVID-19 pandemic in order to fine people not wearing face masks, or more generally to issue traffic fines.[337] During the lockdown, one activist was required by the police to remove his mask so they could take his picture, with no further explanations; he took this case to court in 2022 with the support of the Internet Freedom Foundation, but the judgement is still pending.[338] The Hyderabad police have also been reported to use facial recognition for a number of other purposes, including

cordon and search operations, drug profiling or illegal phone searches,[339] and detaining people who roam around the streets late at night.[340]

In 2020 and 2021 there were reports that the government was planning to roll out a "Smart Governance Programme", known as Samagram. It is supposed to combine several datasets in order to provide the government with a comprehensive "360 degree view" of every resident (such as, for example, when they change jobs or get married).[341] However, there is no official information on the programme and its current status, including the role of biometric information in it. In 2020, the Telangana state government tested the use of facial recognition software for local elections in 10 polling stations in order to identify the voters.[342]

Another Indian city that has earned a place on the "most surveilled list" is Delhi.[343] The Delhi police have publicised the role of facial recognition technologies in making arrests. At the time of the purported riots in 2020, while then-US President Donald Trump was visiting India, arrests of alleged rioters drew special attention. This was at least in part because the arrested people were mostly Muslim, which raised suspicion of the arrests being politically-motivated. The police denied these allegations. The Delhi police commissioner announced that during the riots, the police had recovered and analysed a total of 945 video recordings, 231 people were arrested on the basis of such CCTV or video footage, and 137 of those people were identified through the use of FRT, while in his words "many rioters were identified on the basis of the clothes they were wearing."[344] According to research from the Internet Freedom Foundation, the Delhi Police treat all matches above 80% similarity as positive results.[345]

The use of facial recognition in protests has also been reported in the northern state of Uttar Pradesh, and according to the statement from state police, they are using the technology only to identify targeted people, and do not have or store any protesters' data.[346] Based on similar claims in the EU context, which as mentioned earlier in this book were debunked by the Italian data protection authority, we should be very wary of such claims that these systems are targeted. The very use of such a system at a protest is in itself likely to amount to biometric mass surveillance, and in particular creates a high risk of a "chilling effect" on people's legitimate rights and freedoms to protest.

The use of facial recognition at airports is also present as part of a national pilot which is currently run on a voluntary basis. According to official

statements, the passenger's ID and travel credentials are stored in a wallet on the passenger's smartphone itself, and there is no central data storage, while blockchain technology is used to secure the data, which will be deleted within 24 hours of use.[347] However, this pilot has raised concerns because without a "data protection regime and robust surveillance reform", there are no sufficient guarantees that the data collected and processed for this purpose are not misused.[348]

On the national level, the National Crime Records Bureau (NRCB) initiated a procedure for the creation of a National Automated Facial Recognition System (AFRS) in 2020.[349] At the time of writing, this project is still not completed, but according to a request for proposal issued by the NRCB, this database is purported to be used to "swiftly identify criminals by gathering existing data from various other databases".[350]

When it comes to the private sector, the Indian government recently took steps to allow banks to use facial recognition as well as iris identification for certain banking transactions.[351]

Information on the Indian national ID scheme, Aadhaar, can be found below in the case law section of the book.

LAW

Until 2023, India did not have a comprehensive personal data protection framework or a data protection authority.[352]

In 2019, a draft Personal Data Protection Bill was issued and, after three years of public discussion and debate, withdrawn in 2022 (receiving 81 amendments and 12 recommendations, which made it clear that there was far from public consensus on this text of the law).[353] A new version of the law was proposed in November 2022.[354] Finally, the new law, titled the Digital Personal Data Protection Act (DPDPA), was passed in early August 2023,[355] and to a large extent reflects the 2022 draft.[356]

Although four years passed since the initial text of the DPDPA was prepared in 2019, the acceptance of the final version was described by human rights organisation Access Now as "hasty", while the organisation's representative stated that "the fact that the government rushed the legislation through parliament in barely a week, amidst walkouts, calls for further consultation,

and requests to address surveillance reform is a disservice to the people of India and our democracy".[357]

The DPDPA does not set a date for when it will come into force. The Central Government has ten months to determine the exact dates when the bill's various provisions will become effective.[358] The bill also empowers the Central Government to establish the Data Protection Board of India.

Until the DPDPA comes fully into force, relevant data protection rules are to be found in the Information Technology Act, 2000 (the IT Act)[359] and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the SPDI Rules).[360] These two pieces of legislation constituted the core of the Indian data protection legal framework for a number of years, in expectation of the new and modern law, although their rules are limited in scope and do not address the use of personal data for law enforcement purposes. The IT Act primarily provides legal recognition for transactions carried out using electronic data interchange and other means of electronic communication, and regulates electronic filings of documents with government agencies. SPDI Rules are issued by the government under the IT Act as further clarification.

The DPDPA received critiques for various reasons,[361] including for a general lack of necessity and proportionality requirement for any restriction on the right to privacy — that could "set [it] up for failure in any legal challenge given its clear contradictions with the Indian Supreme Court's *Puttaswamy* judgement in 2017"[362] (for detail about this judgement please see the following section of the study). From the perspective of the topic of this study, the most significant concerns seem to come from the rules around exceptions that the bill provides for government practices, the weak supervisory authority regulated in the bill, and the lack of rules around any data that could be deemed sensitive, including biometrics.

Namely, the DPDPA does not differentiate between any types of personal data, nor does it grant any special protection to data that would be considered sensitive in common modern data protection laws. This is also a significant change when compared to logic behind the IT Act and SPDI Rules. The SPDI Rules set out a definition of biometrics as technologies that measure and analyse human body characteristics, such as "fingerprints", "eye retinas and irises", "voice patterns", "facial patterns", "hand measurements" and "DNA" for "authentication purposes". Biometric information is defined as

a type of sensitive information, provided that such information is not freely available or accessible in the public domain (i.e. such public information would not be considered to be sensitive under the SPDI Rules). There are no rules regulating biometrics specifically within the SPDI Rules.

The SPDI Rules set out various requirements when it comes to processing sensitive information, such as: (i) a privacy policy must be provided with the minimum elements regulated in the SPDI Rules; (ii) collecting data must be done based on the written consent (including electronically) of the data subject and can be withdrawn at any time; (iii) sensitive data are not to be processed unless they are collected for a lawful purpose connected with a function or activity of the organisation that processes them and the collection is considered necessary for that purpose; (iv) an organisation holding sensitive data shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force; (v) any incorrect data must be corrected or amended as feasible; and (vi) sensitive data may be exported outside India, shared with third parties or published only in line with the SPDI Rules.

From the text of the SPDI Rules, it seems evident that they were not well suited to regulate the usage of facial recognition technologies for law enforcement or any other government purposes. Having any type of consent as the legal basis for FRT use by law enforcement agencies is simply not realistic. Many jurisdictions have taken the GDPR, or more generally European, approach and have listed consent as a possible pre-condition or legal basis for data processing. However, not all of them have strict rules around the quality of such consent (e.g. that it has to be freely given and can be withdrawn at any time). One such law is the SDPI Rules, so it can be argued that consent within this legal regime can be implied, instead of expressly given. Nonetheless, it is hard to imagine a scenario in which Indian citizens would "consent" to the use of their biometric data for law enforcement-related purposes.

However, the DPDPA does not seem to rectify this problem in a satisfactory manner. The bill does have more elaborate rules around the legal basis for processing personal data than the SPDI Rules. It maintains that consent is the "primary"[363] legal basis for personal data processing — at least when it comes to private data "fiduciaries" (a term for data controllers under the

bill). If consent is not to be used, an alternative legal ground is one of the limited "legitimate uses" that are defined in the DPDPA .

These legitimate uses cover various public purposes, including processing "for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State".[364] This legitimate use is drafted in very general terms, and thus raises the risk of being used as a "carte blanche" by public bodies for any processing, which is even more concerning due to the above-mentioned lack of proportionally and necessity principles in the DPDPA.

When it comes to the processing of biometrics by law enforcement authorities, even more concerning is the fact that the DPDPA provides for an exception from the bill's application, according to which the Central Government may decide that none of the bill provisions applies to certain government bodies or agencies, if this is "in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these."[365] Again, this exception is not limited by any requirements of necessity or proportionality.

This means that, effectively, the government can exempt all uses of biometrics by law enforcement agencies for any of these purposes from any data protection mechanisms that the DPDPA regulates. The exception was called "near-absolute" by media associations,[366] while the former Supreme Court judge stated that this rule is a "great concern" and that it "gives too much margin to the government and does little to protect individuals' fundamental right of data privacy".[367]

These concerns are further raised due to a lack of effective enforcement mechanisms in the DPDPA. The Data Protection Board of India is not an independent entity but a government-appointed body with limited powers (to issue certain decisions in individual cases as an adjudication body). Its powers do not include the authority to issue any guidance or opinions in the context of DPDPA interpretation.[368]

When it comes to Indian legislation relevant to the use of facial recognition tools for law enforcement purposes, the New Indian Criminal Procedure (Identification) Act (CPIA), 2022 should be mentioned. This law was adopted in April 2022, replacing the Identification of Prisoners Act, 1920

(PA), which was in force for over 100 years. The CPIA does not seem to regulate biometric identification explicitly.[369] However, within the CPIA definition of police "measurements", photographs are included, along with finger impressions, palm-print impressions, foot-print impressions, iris and retina scans, physical and biological samples and their analysis, and behavioural attributes, including signatures and handwriting. These measurements are very similar to the examples usually listed in relation to biometric processing. However, we can only speculate whether "photographs" are meant to include facial recognition, or in the CPIA terminology "face-impressions". The PA defined "measurements" only as finger impressions and foot-print impressions. In addition to such measurements, the police could also take "photographs" of people under the conditions regulated in the PA. For some reason, the term "photograph" from the PA has not been updated in the CPIA to include wording which would indicate photographs can amount to the processing of biometric data derived from such photographs (also because the other "measurements" from the CPIA clearly point to biometric data).

In response to freedom of information requests filed by the Internet Freedom Fund in 2020 and 2021, the Delhi Police replied that they are relying on the provisions of the PA as a legal basis for data processing when using facial recognition.[370] Such a position adopted by the Delhi Police is legally problematic because, in the PA, taking photographs was limited to persons who have been convicted, are out on bail, or those charged with offences punishable with rigorous imprisonment of one year.[371] Now that the PA has been replaced by the CPIA, this legal reasoning still has not changed — "measurements" under the CPIA can be taken only towards a limited scope of persons in the course of criminal investigation, and do not allow for indiscriminate mass surveillance of the whole population in public spaces.

CASE LAW

The most significant case law regarding biometric systems in India was in relation to Aadhaar. According to the official website of the Unique Identification Authority of India (UIDAI),[372] an Aadhaar number is a 12-digit random number issued by the UIDAI to the residents of India who go through the verification process. Any resident of India may voluntarily enrol to obtain an Aadhaar number, and if they are willing to enrol, they have to provide "minimal" demographic and biometric information. This

minimal biometric information includes ten fingerprints, two iris scans, and a facial photograph. According to the same source, the Aadhaar identity platform is one of the key pillars of "Digital India", wherein every resident of the country is provided with a unique identifier.

In its more than ten-year history, Aadhaar went from being a national identification scheme, to the largest national identification database. In 2017, it was described as "the most sophisticated ID programme in the world"[373] — at the time it had 1.123 billion enrolled members, and by November 2022 there were 1.352 billion Aadhaar numbers generated.[374] Initially, it was used for government purposes, but private entities such as banks and mobile operators have subsequently started requiring Aadhaar authentication for access to their services.[375]

In 2017, India's Supreme Court issued a landmark judgement, declaring that privacy in India is a fundamental right, thus overturning two previous judgements that declared the opposite.[376] At the time, it was argued that the judgement would have immediate implications for the government's vast biometric identity scheme, Aadhaar. A ruling on the validity of the scheme (i.e. on the constitutionality of the "Aadhaar Act" that governs the scheme) was expected to be issued next year from a smaller bench of the Supreme Court, so the sentiment was that this 2017 judgement would lead the court toward the invalidation of the Aadhaar. Ultimately, that did not happen.

Aadhaar has been subject to several court rulings over the years. In 2013, the Supreme Court issued an interim order saying that the government cannot deny a service to a resident who does not possess Aadhaar.[377] In 2015, the same court ruled that the Aadhaar unique identity system will not be compulsory for Indian citizens to benefit from government services.[378] Lastly, in the 2018 judgement, the Supreme Court's smaller bench of five judges upheld the constitutional validity of the Aadhaar scheme by a three-judge majority (with one dissenting judge stating that the project "in its entirety is unconstitutional").[379]

The 2018 judgement does, however, impose some limitations on how the scheme can be used. Private businesses and individuals are no longer permitted to ask for an individual's Aadhaar details, which means it cannot be a requirement for services such as opening a bank account, establishing a mobile phone connection or for school admissions. On the other hand, the government is allowed to make Aadhaar details mandatory for tax purposes and welfare payments.[380]

Most notably from the perspective of law enforcement uses, the judgement affected the so-called "national security exception". The exception is regulated in Section 33(2) of the Aadhaar Act. Before the 2018 judgement, it allowed the disclosure of information, including identity information or authentication records, made in the interest of national security,[381] i.e. it effectively allowed investigative agencies to access Aadhaar data without a court warrant.[382] While the judgement did not question the need for the "national security exception" to exist, it did rule that determination of whether national security interests are present in a concrete case should be: (i) made by an officer higher than the rank of a Joint Secretary, which is an executive government position, and (ii) "associated with" a Judicial Officer (and preferably a sitting High Court Judge). The judgement struck down Section 33(2) of the Act in the present form, "with liberty to enact a suitable provision" on the lines suggested above, i.e. with court involvement.[383]

However, in 2019 the amendments to the Aadhaar Act were adopted and only requirement from point (i) above was enacted, requiring the "national security" situation to be determined by someone at the position of a Secretary (which is higher in government hierarchy than Joint Secretary), completely omitting court involvement. Therefore, it can be assumed that the "improved" Section 33(2) of the Aadhaar Act would likely again be declared unconstitutional on the grounds of lack of requirement from the said point (ii).

According to a press release from 2022, UIDAI has developed a face authentication system and mobile app AadhaarFaceRd, to enable Aadhaar Authentication User Agencies (AUA) to capture the face of a person to carry out user authentication,[384] a term which usually relates to confirming a person's identity in order to gain access to a service. On the UIDAI website there is a video instruction on how to use the app for these authentication purposes.[385]

KENYA

What type of act regulates processing of biometric data

National constitution
Yes, the right to privacy.

Data protection law
Yes, the Data Protection Act, 2019.

Bylaws
Yes.

Guidelines
Yes

Defining and regulating facial recognition

Data obtained through facial recognition is defined as biometric data.

Details

Specific use cases defined
- The use of sensitive and biometric data is generally forbidden, allowed only if exceptions apply.

Specific authorities defined
- The Data Protection Commissioner serves as a supervisory authority; it can issue opinions and guidance, handle complaints, run investigations, and impose fines.

Specific conditions defined
- Under prescribed conditions, there is an obligation to register processing activities with the Data Protection Commissioner and/or to appoint data protection officer and/or to conduct data protection impact assessment.

KENYA

CONTEXT

According to a 2021 report prepared by the Institute of Development Studies, Kenya has a long history of government surveillance activities that were spurred in recent years, in part, by a push for anti-terrorism, anti-money laundering, and public health measures.[386] This desire for increased public surveillance by the government seems to be gaining momentum,[387] accompanied by state plans to step up the processing of biometric data, including via the use of FRT.

In 2019, legislation was introduced to regulate the National Integrated Identity Management System (NIIMS), which resembled the ABIS project in South Africa and the Aadhaar system in India. Once established, the NIIMS would have been a "single source of personal information of all Kenyans, as well as foreigners resident in Kenya".[388] Each person in the system should have received a personal identification number called "Huduma Namba". Prior to accessing government and private services, the number would have been necessary for identification, along with biometric templates such as fingerprints as well as pictures of the face, earlobes and iris.[389]

However, in 2023 this project was abandoned by the new Kenyan government and president elected in 2022. In January 2023, President William Ruto announced a plan to have a new digital identification scheme within 12 months, stating that it is not the work of the government to issue IDs but to identify Kenyans.[390] In May 2023, government officials stated that the new implementation deadline is March 2024, and the main purpose of the identification scheme is "to facilitate optimum consumption of government services".[391] Plans to include biometric identification features in the

scheme were expressed by officials in the ID4Africa Augmented meeting held in May 2023. According to these plans, the government will upgrade the currently existing automated fingerprint identification system (called "AFIS") to include iris and facial recognition, which would result in the creation of an "automated biometric identification system".[392] Furthermore, the idea for this eID scheme is to enable machine-readable chip and QR code features to have the possibility of a web-based ID authentication, while the whole scheme would be linked to a new national ID number called the Unique Personal Identifier, or "UPI".[393] "Security threats"[394] and "identity theft" risks are also claimed to be behind these new plans, which should be achieved by "consolidating and digitising existing databases" that are in government control.[395] Therefore, there are some grounds on which to claim that there are "function creep" risks associated with this whole project, as the government can proclaim new purposes for such a comprehensive identification system throughout its implementation, or even at a later phase once all the data has been gathered and the databases linked. These concerns are also based on the fact that President Ruto was "vigorously opposing the Huduma Namba" pre-election,[396] but now that the new identification scheme is being designed, there is no public explanation as to how it will be distinct from the NIIMS.

The year before, in 2018, it was announced that the Kenyan police force had launched FRT on the urban CCTV network, as part of the Critical Incident Management Suite (CIMS) monitored by the Directorate of Criminal Investigations.[397] This FRT deployment involved the installation of thousands of cameras along major roads and highways,[398] focused on Nairobi and Mombasa streets and airports.[399]

In addition to these alleged security and crime-reducing motives, there are also initiatives aimed at fraud prevention. According to publicly-available information, in a dispute about the necessity of installing equipment to biometrically register and verify patients and submit e-claims for payments, 850 hospitals sued Kenya's National Hospital Insurance Fund (NHIF) in 2021.[400] The NHIF claimed that the mass biometric registration aims to tackle fraud and to speed up the payment of medical claims. If this project is implemented, hospitals would be expected to verify patients' identities with a fingerprint recognition scan, instead of requiring patients to present an ID or membership card.[401] There is no available information on the outcome of this dispute.

A significant national case involving FRT in the private sector involves the telecommunications company Safaricom, which required their customers to re-register by using this technology. The reason was that the Communication Authority of Kenya (CA) demanded mobile services operators to register their customers afresh, as a measure to drive out criminals.[402] Safaricom thought that this meant they could use facial recognition registration as a security measure. However, the international human rights organisation Access Now reacted with a public letter in which it stressed that this Safaricom data collection was in violation of the Kenyan Data Protection Act, and called for data deletion.[403]

LAW

Article 31 of the Bill of Rights enshrined in the Kenyan Constitution protects the right to privacy, which includes the right not to have information relating to a person's family or private affairs unnecessarily required or revealed.[404]

The Kenyan Data Protection Act (KDPA) 2019 came into force on 25 November 2019.[405] Soon after, several bylaws called Regulations were issued by various competent bodies to regulate specific matters.[406] A supervisory authority called the Data Protection Commissioner (simply referred to as the Commissioner) was appointed on 16 November 2020.[407] So far, the Commissioner has been active in providing guidelines on specific topics, none of which are directly related to the processing of biometric data.[408] The legal landscape is in large parts modelled after the EU data protection tradition and structure.[409]

As in the case of the South African law, the KDPA regulates exceptions, i.e. situations when processing of personal data is exempt from the provisions of the Act. One of these is the same as in the GDPR — provisions do not apply to processing of personal data by an individual in the course of a purely personal or household activity. Two other Kenya-specific exceptions are: (i) if the processing is necessary for national security or public interest; or (ii) disclosure is required by or under any written law or by an order of the court. These are both relevant to law enforcement processing of biometric data, but there remains the issue of which laws are applicable to these situations. Such processing would, therefore, have to be regulated by some other legal provisions in the Kenyan legal system. Furthermore, the KDPR expressly regulates that even when exceptions are applicable, no data controller or data processor can be exempt from complying with data

protection principles relating to lawful processing, minimising collection, data quality, and adopting security safeguards to protect personal data.

The KDPA defines biometric data as personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, earlobe geometry, retinal scanning and voice recognition. As in South Africa's POPIA, facial recognition is not mentioned explicitly, but should fall within the scope of the definition as it is physical characterisation. Biometric data are further covered by the definition of "sensitive personal data".

The basic logic of the KDPA is that only special types of processing activities must be registered. The Commissioner has the mandate to prescribe thresholds required for mandatory registration, while the KDPA indicates that for this purpose the Commissioner must consider whether sensitive personal data is being processed. According to the Data Protection (Registration of Data Controllers & Data Processors) Regulations (2021), the registration threshold is primarily set based on the annual turnover of controllers and processors.[410] However, there is a list of processing activities whose registration is mandatory regardless of the turnover, and these include, inter alia, "crime prevention and prosecution of offenders (including operating security CCTV systems)" and "businesses that process genetic data".[411] But, with the exception of DNA, biometric data are not singled out.

Pursuant to the KDPA, in cases when the core activities of the data controller or processor consist of processing sensitive categories of personal data, they must appoint a data protection officer (DPO). Provisions that regulate the position and duties of the data protection officer are very similar to those in the GDPR. There is no publicly-available information on whether any relevant controllers have appointed their DPOs to oversee the processing of biometric data.

Any sensitive personal data can be processed only if there is a special legal ground regulated in Article 45 of the KDPA, subject to fulfilment of the data processing principles. Here again, the logic is very similar to the GDPR. Additionally, the Commissioner can specify any further grounds on which such sensitive data may be processed. None of these legal grounds regulates the processing of biometric data specifically, so the general regime for sensitive data continues to apply.[412]

The transfer of sensitive data outside Kenya is allowed upon obtaining the consent of a data subject and confirmation of appropriate safeguards by the Commissioner, according to Article 49 of the KDPA.[413]

Rules on automated decision-making from the KDPA are very similar to GDPR ones, and even more detailed than those from Article 22 of the GDPR in some aspects. According to Article 35 of the KDPA, the data subject must be informed that a decision about him or her is made solely on automated processing. The data subject can then request the controller or the processor to (i) reconsider the decision; or (ii) take a new decision that is not based solely on automated processing. Furthermore, after receiving such a request, the controller or processor must inform the data subject of the steps taken to comply with the request and the outcome of complying with the request, by notice in writing.

Some rules on the processing of biometrics and other sensitive data can be found in the respective Regulations issued so far. The Data Protection (General) Regulations (2021) regulate that data, subject to fulfilment of other conditions regulated in the KDPA,[414] can be collected from "biometric technology, including voice or facial recognition".[415] According to Article 49(1)(c) of the same Regulation, the preparation of a Data Protection Impact Assessment (DPIA) is mandatory in the case of processing biometric data.

The Commissioner has issued a number of guidance papers, including on the preparation of a DPIA. None of the papers issued so far addresses specific matters relating to biometric data or FRT.[416]

Kenya now seems to have a modern and robust legal framework for the processing of personal data and various legal instruments aimed at addressing the higher risk arising from the processing of sensitive data, including biometrics. Some concerns remain, given that biometric data do not have any special protections directed at their collection and use. Since these rules came into force rather recently, it remains to be seen whether these laws will be able to address the relatively widespread use of biometric systems.

A ruling of the High Court of Kenya in the Huduma Namba dispute and the Commissioner's willingness to issue high penalties are encouraging steps for the rule of law, as is explained in the next section.

CASE LAW

There have been two important decisions regarding the NIIMS made by the High Court of Kenya.

As mentioned, in 2019 the Government planned to establish the NIIMS. Under the laws issued for that purpose, Kenyan citizens and foreign nationals are required to contribute sensitive personal information, while all of them were to obtain a unique identity number known as Huduma Namba. This initiative was met with strong opposition from the outset, for various reasons including privacy concerns.[417]

On 30 January 2020, the High Court decided on the petition of three applicants, declaring that the collection of DNA and GPS coordinates for the purpose of identification under the NIIMS was "intrusive and unnecessary".[418] Although the collection of other biometric data was not excluded on similar grounds, the overall conclusion was that the legal framework on the operations of the NIIMS was "inadequate, and poses a risk to the security of data that will be collected in the system".[419] Under these circumstances, the Court ruled that the Government can proceed with the implementation of the NIIMS only on the condition that there is an appropriate and comprehensive regulatory framework for its implementation, compliant with the applicable constitutional requirements.[420]

The following year, in a decision issued on 14 October 2021, the High Court held that the KDPA applied retroactively to the NIIMS, in response to an application that sought to suspend the implementation of the Huduma Namba card in the absence of a DPIA.[421] To justify this reasoning, the Court stated that "since the state chose to put the cart before the horse, so to speak, it has to live with the reality [that] there now exists legislation against which its actions must be weighed irrespective of when they were taken so long as those actions touch on the individual's right under Article 31 of the Constitution [...]".[422] In this ruling, the government's decision to implement the Huduma Namba cards was quashed by the High Court, albeit temporarily, as it was ordered to conduct a DPIA before continuing the implementation process.[423]

We shall see how this judgement impacts plans to establish the "automated biometric identification system". The government claims that they have learned their lesson,[424] although currently there is no official information

on which legal rules would be enacted in relation to the new identification scheme in order to provide safeguards required by the High Court. In May 2023, nine human and digital rights groups issued a public statement highlighting the need for transparency, public engagement and respect for legal rules (including securing the proper legal basis and preparing appropriate impact assessments) as prerequisites for new ID scheme deployment.[425]

According to publicly-available information, there are no other court judgements regarding FRT uses at the time of writing this report, including by the police and other government agencies for safety reasons.

However, the Commissioner issued a first penalty for a violation of the KDPA in December 2022.[426] The penalty was issued to a company that infringed the privacy of a complainant by using their photo on the company's Instagram account without the complainant's consent, as well as subsequent violations of their KDPA obligations, including lack of cooperation with the Commissioner. For this violation, the company was fined KES 5,000,000, which is equivalent to approximately EUR 36,000 – the highest penalty available under the KDPA. This decision is subject to appeal, but it indicates the Commissioner's willingness to impose strict fines in its efforts to secure a strong application of the KDPA.

LATIN AMERICA

What type of act regulates processing of biometric data

National constitution
Yes.

Data protection law
Yes. Numerous countries have enacted data protection laws, many of which influenced by the European Union's legislation.

Guidelines
Yes.

AI Regulation
Yes. Brazil published a draft law in 2022.

Local level legislation
Yes. Buenos Aires legalised facial recognition by amending an existing security systems legislation.

Defining and regulating facial recognition

Facial recognition is explicitly defined in Brazil.

Data obtained through facial recognition is defined as biometric data in numerous countries.

Details

Specific use cases defined

- Biometric data must be collected from anyone entering Argentina for security purposes.
- There are laws regulating the use of facial recognition technology at stadiums and in the inter-municipal transportation system in Brazil.
- A bill in Colombia allows the National Civil Registry to use various biometrics for identification and authentication.

Specific authorities defined

- The final version of the Brazilian AI law is expected to define specific conditions for the processing of biometrics.

LATIN AMERICA

CONTEXT

Numerous Latin American countries have implemented biometric technologies for surveillance, usually presented by public officials as a technological advancement to fight crime and enhance public safety.[427] These technologies have been deployed without proper legal grounds, human rights assessments or transparency, and have been used for purposes beyond public safety — even for spying on political adversaries.[428] There is a lack of specific regulations for their use, raising concerns about the violation of privacy and other human rights, as well as a lack of avenues for redress. The technologies also heavily rely on police databases that can reinforce and exacerbate the discriminating ways in which they have been compiled, while data use standards are not well-defined.[429]

Although the region has transitioned to democratic procedures, an authoritarian political culture continues to exist in some ways, as demonstrated by heavy-handed repression of protesters by the state in countries such as Venezuela, Ecuador and Chile.[430] The deployment of facial recognition and other biometric technologies in this context further amplifies the risks and concerns.

While several Latin American countries share many similarities in the adoption of biometric surveillance technologies, Argentina and Brazil have seen the most significant adoptions of biometric technologies and are therefore the focus of the following chapter. The introduction of the Federal Biometric Identification System for Security (SIBIOS) in 2011 marked a significant turning point in Argentina for the adoption of a system which could enable biometric mass surveillance.[431] Under SIBIOS, biometric data — including fingerprints, palm prints and face photos

— must be collected from every citizen and anyone entering the country. End-users of SIBIOS, such as police officers and border agents, are not required to obtain a warrant or judicial authorisation to access the biometric database. The lack of legislative debate and limited consultation with non-governmental entities regarding the implementation of the system has kept it away from public opinion. This has resulted in low awareness of the risks associated with the extensive collection of private data by the state.[432]

In the last decade, the use of biometric technologies has expanded rapidly in Argentina, being utilised not only for purported public safety and immigration purposes, but also for identity verification in areas such as social security programmes, banking, taxes, education, elections and sports.[433] Buenos Aires, the capital city of Argentina, employed live facial recognition in the city's train stations, with cameras both within the stations and facing the street. The system, presented as a way to capture individuals listed in the country's national fugitive database, was used between 2019 and 2022.[434] Numerous "false positive" cases were reported, emphasising the fact that the technology is flawed, prone to errors, and can lead to serious violations of fundamental rights.[435] The use of the technology was temporarily suspended and subsequently deemed unconstitutional by a city court.[436]

Biometric technologies, including facial recognition, are widely used in Brazil's public and private sectors. There are frequent implementations of facial identification in public spaces and events with the excuse of addressing high levels of violence and crime.[437] Biometric verification is also used for fraud detection in accessing public services and even for school attendance management in educational institutions.[438] There have also been cases of gender, age and emotion recognition for marketing purposes, although some projects have faced legal challenges.[439]

The National Civil Identification (ICN) system in Brazil aims to collect the biometrics of the entire electorate by 2026.[440] It involves a centralised database called the ICN Database (BDICN), which combines various existing government databases, including the biometrics register of the electoral system. As of June 2022, 130 million users were biometrically registered to vote, making up a significant portion of the population. There are concerns about the risks associated with the ICN system. These risks fall into two categories: risks related to the system's information architecture and governance arrangements, including potential abuses of personal data, and

risks of excluding citizens due to the use of the BDICN for authenticating users on the gov.br platform.[441]

Regarding the use of biometric technologies at the borders, civil society groups in Latin America have called for the termination of cooperation agreements made by Mexico, Guatemala, Honduras and El Salvador with the United States, which allow for cross-border transfers of biometric and other types of personal data of people on the move.[442] These data-sharing agreements have raised serious concerns about privacy invasions, discrimination and arbitrary decision-making. Civil society organisations that are advocating for the termination of these agreements have also been urging for the inclusion of safeguards to protect the privacy and data of people on the move, such as prohibiting data processing without local data protection laws, preventing profiling and predictive analysis, and limiting access to data. Special protections for children, the requirement for informed consent, and rights to access, rectification, deletion and objection are also recommended.

Different approaches have been proposed to address the risks associated with facial recognition technology in the region. Some advocate for moratoria until proper safeguards are in place, while others call for comprehensive bans on its use for law enforcement purposes in public spaces.[443] Several civil society organisations also call for robust safeguards, including remedies for privacy violations and enhanced accountability and transparency by both technology companies and government authorities.[444]

Since 2022, the civil society-driven campaign *#SaiDaMinhaCara* ("Get out of my face") has encouraged 50 state and municipal legislators in Brazil to introduce proposals to ban facial recognition from being used in public spaces.[445] Their concerns include biassed outcomes, wrongful arrests, and the reinforcement of racial discrimination. The initiative highlights the risks of mass surveillance and the erosion of privacy in public spaces. It is led by organisations specialising in technology, security and human rights, collaborating with parliamentarians to push for legislative restrictions.

LAW

Numerous Latin American countries, such as Chile,[446] Uruguay,[447] Mexico,[448] Costa Rica,[449] Peru, Brazil, Panama and Ecuador have enacted data protection laws, many of which were influenced by the European

Union's GDPR model. However, it is worth noting that certain countries in the region, such as Venezuela and Bolivia, still do not have data protection laws.[450]

A significant challenge with the regulation of biometric technologies across the region is that a large number of countries with specific data protection laws have not updated them adequately to address the challenges posed by current digital technologies. In some countries where general rules on personal data protection exist, specific regulations pertaining to the use of biometric data are lacking. For example, in a report that mapped 38 initiatives for the use of facial recognition in Latin America, over 60% of them lacked specific legal bases to support the implementation of the technology that had already been rolled out.[451] In some instances, broad interpretations of existing regulations or analogies to other technologies were used to justify its deployment.

There are just a few cases where regulations explicitly address facial recognition or other biometric identification technologies. Examples include a Brazilian regulation enabling biometric data collection for driving licences,[452] regulations governing the Comprehensive Public Video Surveillance System in Buenos Aires,[453] and a bill in Colombia allowing the National Civil Registry to use various biometrics for identification and authentication.[454]

ARGENTINA

Argentina has strong privacy protections enshrined in its national Constitution (Articles 18 and 19)[455] and has ratified international human rights treaties. It has a robust but outdated data protection regime in Article 43 of the Constitution and the Personal Data Protection Act 25.326 (PDPA),[456] passed in 2000. Argentina is also recognised by the European Commission as a country that ensures an adequate level of data protection. However, these laws have proven insufficient in protecting citizens from state surveillance, since the government has used legal exceptions to deploy surveillance programmes for a wide range of reasons including state functions, improving services, and purported public safety.

The deployment of facial recognition technology in Buenos Aires, for example, initially lacked a proper legal framework and was introduced through a city government resolution rather than a law. However, in October

2020, the city legislature legalised its use by amending an existing security systems legislation: Law 5688 (2016).[457] Civil society organisations strongly opposed the amendment, arguing that proper human rights assessments, especially regarding the right to privacy, were not conducted.[458] The UN Special Rapporteur on the right to privacy also expressed concerns about the deployment of facial recognition in Buenos Aires, in particular the lack of privacy impact assessments and adequate safeguards.[459]

Argentina's outdated data protection law, established in 2000, has also been a point of contention regarding facial recognition deployments. Civil society groups have called for an update to the law to provide clear guidelines and protections for collecting sensitive personal data through technologies like facial recognition.[460]

In November 2022, the Argentinian data protection authority (AAIP) published a draft bill to update the PDPA, following a public consultation in September 2022.[461] The draft bill introduces new definitions to the Act, including "biometric data", which are only considered to be sensitive if they can reveal additional information, the use of which may potentially result in the discrimination of the data subject. Resolution 4/2019 ("the Biometric Guidelines") issued by the AAIP, provides examples of such sensitive data, including ethnic origin and health information.[462] However, this additional requirement for biometric data reduces the level of protection for data subjects compared to other regulations that govern the use of biometric data, such as the GDPR.

Compared to the GDPR, the PDPA's consent condition for processing sensitive data also does not provide strong enough protection for data subjects. Given the increased risks associated with processing sensitive data, experts have pointed out that explicit consent should be required.[463]

BRAZIL

Brazil has established a legal framework to protect the right to privacy, including enshrining privacy as a fundamental right in the federal Constitution,[464] and recognising international human rights treaties. The country also has specific legislation, *Marco Civil da Internet* (Civil Rights Framework for the Internet), which safeguards privacy in the online context.[465] Additionally, Brazil has implemented the federal data protection law *Lei Geral de Proteção de Dados Pessoais* (LGPD), which entered into

force in September 2020. The LGPD attempted to unify over 40 different statutes that previously governed the use of personal data in Brazil, and to set modern standards for data protection.[466] In October 2021, the Brazilian Senate unanimously approved the Proposed Amendment to the Constitution (PEC) No. 17/2019, which acknowledged the protection of personal data as a fundamental right in the Brazilian Constitution.[467]

While the LGPD is considered one of the most progressive data protection laws in the wider Latin American region, it does not have a specific definition of biometric data, leaving space for legal loopholes and exploitation. It also sets explicit exceptions for activities related to public safety, national defence, state security, and the investigation and prosecution of criminal offences. That means that facial recognition used by public security forces falls outside the LGPD's protections. Efforts are underway to regulate data protection in law enforcement, with experts proposing a draft "Criminal LGPD" bill to establish data protection principles and obligations for law enforcement authorities.[468] However, it is uncertain when this will be enacted.

In the context of private companies involved in deploying facial recognition systems, such as in São Paulo's privately-run public transport system, the protections of the LGPD, the provisions of the Marco Civil da Internet, and the Consumer Protection Code apply.

Numerous state laws are directly addressing facial recognition technologies. For example, three specific laws regulate the use of facial recognition technology in stadiums: Law No. 16.873/2019 in Ceará,[469] Law No. 21.737/2015 in Minas Gerais,[470] and Law No. 8.113/2019 in Alagoas.[471] Additionally, Law No. 7.123/2015 in Rio de Janeiro focuses on the deployment of facial recognition technology in the inter-municipal transportation system.[472] However, these laws do not contain sufficient legal safeguards for deploying the technology.

Law nº 6.712/2020 regulates the use of facial recognition for public security purposes in the Brazilian capital but falls short in terms of cybersecurity protections and data subject rights.[473] It also allows for the technology's use in criminal investigations. The Ministry of Justice and Public Security has issued a directive promoting the implementation of facial recognition systems and other surveillance technologies.

In December 2022, a committee of the Brazilian Senate presented a report and a draft artificial intelligence (AI) law aimed at regulating AI in the country.[474] The proposed legislation categorises AI systems based on risk: biometric identification systems are classified as high-risk AI systems. The competent authority is tasked with creating and maintaining a publicly accessible database of high-risk AI systems, along with the completed risk assessments provided by suppliers and end users.

The law prohibits the use of systems classified in the "excessive" risk category, where it currently puts the use of facial recognition and other biometric identification systems for public security purposes — unless authorised by law or judicial authorisation in cases of crimes in progress or searches for missing persons or crime victims. As pointed out repeatedly throughout this book, such a basis is open to very wide interpretation and there is a risk that it could be used to justify almost perpetual use.

The draft law guarantees various rights, including an explanation of decisions, the ability to contest them, and human participation in the decision-making process. The law also highlights the right to non-discrimination and to correct identified biases.

CASE LAW

In a historic ruling from May 2020, the Brazilian Supreme Court declared the right to data protection as an independent and fundamental right under the Brazilian Constitution.[475] The Court suspended a presidential executive order that required telecom companies to share the personal data of over 200 million individuals with the Brazilian Institute of Geography and Statistics (IBGE) for census research. The decision signified a significant step towards recognising the protection of personal data as a separate right from the right to privacy, similarly to how it is addressed in the Charter of Fundamental Rights of the European Union.

A Civil Court in São Paulo, Brazil, ruled in May 2021 that the use of facial recognition technology on a subway line violated individuals' right to privacy and freedom of information.[476] The subway operator, ViaQuatro, introduced interactive subway car doors that displayed personalised advertisements based on emotion recognition technology. A consumer rights organisation filed a lawsuit seeking damages and an order to prohibit the use of the technology. The Court held that the use of facial recognition or

detection software required user consent and ordered the subway operator to stop using the technology. The Court emphasised the importance of data protection and privacy rights under the *Lei Geral de Proteção de Dados Pessoais* (LGPD). It awarded damages for collective harm, but dismissed the request for damages related to non-economic harm suffered by riders individually, stating that it would duplicate the compensation already granted for collective harm.[477]

In a landmark case for Argentina, a trial judge in Buenos Aires declared unconstitutional the Fugitive Facial Recognition System (*Sistema de Reconocimiento Facial de Prófugos*, SRFP) implemented by the local government.[478] The judge's ruling established a precedent for protecting privacy and fundamental rights in the context of public surveillance for law enforcement purposes. Firstly, it recognised privacy, intimacy and data protection as collective rights, rather than solely individual rights. Secondly, the court determined that civil society organisations had the standing to sue based on the violation of these collective rights. Thirdly, the judge also concluded that an "amparo" action (a constitutional remedy) was appropriate to address the harm caused by the system. The decision highlighted privacy violations and abuse of authority by system operators.

The SRFP had used facial recognition software installed in surveillance cameras — the sort of capability that the Technical chapter of this book has highlighted are becoming increasingly common — to match images against a database of fugitives. Civil society organisations criticised the risks to privacy and other human rights. The court found that the SRFP lacked oversight, led to unlawful detentions, and relied on an unreliable database. The judge also noted misuse of the system and a lack of accountability. The court prohibited the operation of the SRFP until control and oversight mechanisms are established. The decision did not go as far as to declare the law creating the SRFP unconstitutional, but outlined requirements for its future implementation.

In April 2022, Mexico's Supreme Court ruled that a plan to establish a national cell phone user registry with biometric data was unconstitutional.[479] The initiative aimed to combat crime by making it harder for criminals to remain anonymous when purchasing mobile phones. The court recognised the potential human rights violations and security risks associated with collecting sensitive biometric data, including the fingerprints or eye biometrics of approximately 120 million phone users. This ruling not

only protected individuals' privacy but also highlighted the importance of safeguarding personal information in the face of technological advancements.

SOUTH AFRICA

What type of act regulates processing of biometric data

National constitution
Yes, the right to privacy.

Data protection law
Yes. The Protection of Personal Information Act, 2013.

Bylaws
Yes.

Guidelines
Yes.

Defining and regulating facial recognition

Data obtained through facial recognition is defined as biometric data.

Details

Specific use cases defined
- The use of sensitive and biometric data is generally forbidden, allowed only if exceptions apply.

Specific authorities defined
- The Information Regulator serves as a supervisory authority; it can issue opinions and guidance, handle complaints and investigations, cannot issue penalties but can issue administrative fines.

Specific conditions defined
- Under prescribed conditions, there is an obligation to obtain prior authorisation for processing from supervisory authority.

SOUTH AFRICA

CONTEXT

There is no concrete evidence that public bodies in South Africa have used facial recognition technology on the general population. However, there are concerns that this may be the case, or that this technology may soon be widely used.

South African police have been expressing their wish to start using this technology for the last fifteen years.[480] Concerns have also been raised about the presence and activities of the private company Vumacam, which has built a nationwide surveillance network that scrutinises peoples' movements for "unusual behaviour" via their smart surveillance solutions. This state of affairs may be dangerous as it could lead to a slippery slope from behavioural surveillance to facial identification, as the underlying technological systems are the same. Moreover, even though behavioural surveillance without identifying people may seem benign, from a data protection perspective it is still very sensitive. The collection of behavioural data that involves people (not just objects) is, in its essence, a collection of personal data. In combination with other information, such data could lead to the identification of a person, as well as discriminatory profiling. In its most refined form, behavioural characteristics can lead to identification if they can be used as measurable patterns of human activities, in which case they would be considered biometric data.

Vumacam sells its private security services to local companies. It already seems to have a monopoly, which is not only based on the claimed capacities and effectiveness of its technology, but also the company's (unofficial) cooperation with local police. This presumption is based on several case studies regarding

Vumacam's presence and plans in South Africa in the last couple of years.[481] According to these sources, Vumacam's representatives have repeatedly rejected claims that they started using facial recognition in order to provide their services and develop their technology. However, if one looks at the features they already use (e.g. licence plate recognition) they seem to have the technical infrastructure and processing capability to make this possible.

In addition, the South Africa Home Affairs Ministry started their Automatic Biometric Information System (ABIS) project in January 2016.[482] ABIS is intended to provide a single source of identification for South African citizens and non-citizens across state institutions and private sector entities, and would extend the current national identification system (Hanis). According to the statements of public officials, ABIS will contain information such as a person's fingerprint, photo, palm print, facial recognition and iris scans.[483] The system is still not in place, but its implementation seems to be inevitable based on new reports, since one of the main reasons for postponement is problems with a contract that has been concluded with a service provider.[484] In May 2023, the Portfolio Committee on Home Affairs issued a media statement to express disappointment with delays in project implementation and problems with a private contractor on the project; but with respect to the collection of biometrics, they expressed support for "the use of an upgraded system with innovative technological functionalities, such as facial recognition and palm biometric modalities, which will create further confidence in the population register".[485]

Since 2021, the South African government has been implementing the Biometric Movement Control System, or BMCS for short, at the borders. In May 2023, this system was implemented at 34 ports in the country, including major airports.[486] According to the website of South African Airways, "if you are a non-South African citizen, travelling through the ports of entry you will be expected to provide your fingerprints and photograph at the Immigration counter".[487] Other than this practical information, the Home Affairs website offers no other explanation on how this system works.

LAW

The South African Constitution recognises the right to privacy as a fundamental human right.[488] Furthermore, rights to privacy and to the protection of personal data are regulated by the Protection of Personal Information Act 4 of 2013 (POPIA), applicable from 30 June 2021.[489] The POPIA seems to be modelled, to a large extent, on the EU data protection

legal tradition. In compliance with the POPIA, South Africa has a dedicated data protection authority called the "Information Regulator".[490]

Biometrics is defined in the POPIA as "a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition". For some reason, the definition does not explicitly include facial recognition (which is also the case with the law in Kenya, possibly suggesting a common history with regard to this definition). However, as the list is non-exhaustive, there is no reason to consider this definition as excluding facial recognition. Biometric information is considered to be "special personal information", as defined in Article 26 of the POPIA.

With respect to special personal information, its processing is in principle forbidden in the POPIA, unless one of three exception categories apply: general exceptions; an Information Regulator authorisation applicable to any special personal information; or a specific exception which regulates only biometric information.

There are five general exceptions, again with similarities to the EU's General Data Protection Regulation, where processing would be allowed because either: (i) the data subject has given consent; (ii) processing is necessary for the establishment, exercise or defence of a right or obligation in law; (iii) processing is necessary to comply with an obligation of international public law; (iv) processing is for historical, statistical or research purposes (subject to further conditions); or (v) the information has deliberately been made public by the data subject.[491]

In addition, the Information Regulator may, upon application by a responsible party,[492] authorise the processing of special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject. There is guidance issued by the Information Regulator that regulates this authorisation procedure.[493]

Finally, there is a separate exception that regulates the processing of biometric data only.[494] According to Article 33 of the POPIA, the processing of biometric information may be allowed if the processing is carried out by bodies charged by law with applying criminal law, or by responsible parties who have obtained that information in accordance with the law. Therefore, this permission for the use of biometrics by some public bodies

in the POPIA is quite broad and does not regulate any specifics of the biometrics in question. One possible interpretation of this legal rule is that the concrete situations when biometric information can be processed under this exception should, in principle, be further regulated via legal provisions that make these rules operational and concrete (e.g. via a separate law or amendments to existing laws). This would be a similar situation to the legal dynamics between the LED in the EU and national laws in the Member States, in the sense that the former sets the general rules while the latter should regulate use of biometrics for law enforcement purposes in greater detail (inter alia, to establish appropriate safeguards for such processing).

There is still no law in place in South Africa that would regulate processing of data via facial recognition technology or by law enforcement agencies specifically, despite the collection of face data under ABIS.[495] Taking into account that the law enforcement agencies in South Africa still do not claim to use facial recognition in their investigations (nor are there any proofs of such practice), time will show whether Article 33 of the POPIA will be used by them as a legal basis for such use.

Rules around the use of biometrics in criminal procedures should also be interpreted in the light of Article 6 of the POPIA, which regulates exclusions from the law. According to one such exclusion, the POPIA does not apply to the processing of personal information by a public body in situations which involve national security, or when the purpose of processing is prevention, detection and investigation of offences, prosecution of offenders or execution of sentences, but only to the extent that adequate safeguards have been established in legislation for the protection of such personal information. In the absence of any laws that would regulate biometric surveillance for the said purpose, the POPIA does seem to apply (until such rules are in place).

According to Chapter 6 of the POPIA, the responsible party must obtain "prior authorisation" for certain processing activities from the Information Regulator, because of their specific nature. The responsible party that wants to process biometric information (based on appropriate legal grounds) does not, in principle, need to obtain such prior authorisation for the processing itself. However, such authorisation would be needed if data were to be transferred abroad to a non-adequate country. There is also guidance that regulates this authorisation procedure.[496]

The POPIA has rules related to automated decision-making which are similar to their GDPR counterparts, although they seem to be narrower in scope as they focus on decision-making that is based on profiles made via automated processing (Article 71).

Therefore, there are several potential legal grounds for South African public bodies and police that may be used if facial recognition technology is to be implemented in practice in the future. It remains to be seen whether the appropriate legal procedure will be followed in such a case.

CASE LAW

Although it did not concern facial recognition, a significant case about mass video surveillance was finally decided by the High Court of South Africa in 2020.[497] The case was initiated by the Vumacam company against Johannesburg Road Agency (JRA), which had suspended their aerial and CCTV wayleave applications (which give Vumacam the right to access public roads to install their equipment). The JRA justified the suspension decision arguing that Vumacam's aim to install the cameras was "to surveil the movements of 'innocent people' and sell the 'footage' to third parties". According to the wording of the judgement, the essence of the JRA's case is that Vumacam is spying on individuals' movements and thereby infringing their rights to privacy as protected by the POPIA. To cope with the problems that arise from such spying activities, a regulatory framework would have to be established. Such a framework should focus on ensuring that the material collected through the cameras is handled in a manner that protects the privacy of individuals.[498]

However, the argument of the JRA was not accepted by the court. Namely, the decision-making of the JRA is bound by the bylaws applicable to them. Such bylaws do not prescribe the competence of the JRA to suspend any wayleave right based on violations of the right to privacy. In the words of the court, the JRA is an administrative body with no powers outside of those conferred upon it by the law in general, and in this case by the bylaws in particular.[499]

In an interview regarding this court win, the CEO of Vumacam stated: "Our infrastructure is highly beneficial to the public, security companies, to law enforcement and even to the JRA in flagging incidents that may cause damage or harm to roads infrastructure. There are multiple, daily

successes reported where our cameras both prevent crimes and assist in the apprehension of criminals."[500]

This case shows that there is some serious cause for concern in South Africa that the right to privacy may be jeopardised in the name of (promised) security. This risk is recognised even by public bodies such as the JRA, although they lack the competence to challenge the alleged violation of privacy. Once the ABIS database is in place, possibilities for the use of FRT will be greatly increased. It remains to be seen how (and if) POPIA rules will be followed by all the stakeholders.

UNITED ARAB EMIRATES

What type of act regulates processing of biometric data

National constitution
Yes; right to privacy (home and communication).

Data protection law
Yes. The Personal Data Protection Law, 2021.

Defining and regulating facial recognition

Facial images are included in the definition of biometrics, but there are no specific rules on the processing of biometric data.

Details

Specific use cases defined

- The Data Office, a supervisory authority established under the Personal Data Protection Law, will be regulated in detail by Executive Regulations.

Specific conditions defined

- Under the conditions provided by the Personal Data Protection Law, data controllers should appoint a data protection officer and conduct a data protection impact assessment.

UNITED ARAB EMIRATES

CONTEXT

The use of facial recognition in the United Arab Emirates (UAE) is widespread. It is used in both public and private sectors for various purposes, and such a trend is heavily supported by the government.

From a technical angle, proponents and purveyors of biometric technologies have noted that with its diverse population, the UAE is ideal for testing new facial recognition technologies, with more than 200 different nationalities represented in Abu Dhabi and Dubai.[501] For that and a combination of other reasons, many tech companies have been offering their services and products in the UAE market, especially Chinese ones.[502]

One of the UAE government's strategic goals is to become a global leader in artificial intelligence technologies.[503] Part of this strategy is also to build smart cities, including the use of facial recognition in ways that seem likely to amount to biometric mass surveillance. One of the use cases mentioned in the strategy is deploying "facial recognition to monitor driver fatigue".[504]

In 2018, government agencies developed and deployed the "UAE Pass" application.[505] The website states that it is the "first national digital identity and signature solution" that enables users to identify themselves to government and private service providers using their smartphone, thus enabling them to access online services. The application has additional features (that distinguish it, for example, from Aadhaar in India and ABIS in South Africa) as it provides the citizens with tools to sign and authenticate documents and transactions digitally, to request official documents in digital form, and to

request services from UAE pass partners.[506] The app uses facial recognition to register and authenticate users, by creating a "Facial ID".[507] According to public officials, using facial recognition technology in the registration process is "a key step towards the implementation of emerging technologies based on AI, to establish a digital lifestyle in the UAE".[508] In the following years, the UAE pass was linked to Emirates ID, a national ID card.[509]

When it comes to the use of facial recognition by law enforcement agencies, it is widespread in the UAE, including 24/7 live surveillance. There were also reports that Dubai police had plans for pioneering predictive policing tools in their decision-making process, which would be based on biometric data.[510]

According to the UAE government portal, the UAE Ministry of Interior implemented a face recognition system to "protect" the country's borders, critical infrastructure and valuable assets. The system uses "sensitive cameras" (there is no explanation on the government portal about what sensitive cameras are) to capture people's faces. The cameras can scan and take pictures of people standing both close to and far from them and can detect whether they are moving or still.[511]

In 2018, the Dubai Police launched the "Oyoon" AI Surveillance Programme. According to the information provided on their Facebook page at the time, the aim of the project is "to create an integrated security system that works through all strategic partners to exploit modern and sophisticated technologies and artificial intelligence features to prevent crime, reduce traffic accident-related deaths, prevent any negative incidents in residential, commercial and vital areas, and to be able to respond immediately to incidents even before they get reported to the command unit".[512]

Already in 2019, it was claimed by the police that the programme helped with the arrest of 319 suspects in the first year of its deployment. According to these reports, within the Oyoon network, approximately 5,000 security cameras across Dubai relay live images of security breaches to the Central Command Centre, while three sectors are in surveillance focus — tourism, traffic, and brick and mortar facilities. On the other end of the system, the police digitally track suspected criminals just by uploading their mugshots into a database.[513] According to reports from 2022, over 300,000 cameras were linked to the Oyoon network.[514]

In 2020, it was reported that a new facial recognition system will be introduced in Dubai metro stations. Additional features of the system include "smart helmets" and "smart glasses". Namely, according to Dubai police officials, the police's smart glasses called Rokid T1 and the smart helmets that were used during the COVID-19 pandemic to scan commuters' temperatures, will have more "advanced" technology such as facial recognition, which they claim they will use to identify wanted people.[515]

When it comes to Abu Dhabi practices, Abu Dhabi police upgraded their patrol cars with a live facial recognition system in March 2020. The police central operations department server is linked to the cars' smart bar, and the software can instantly cross-reference an image with the police watch list. Police are alerted to take action when there is a match.[516]

This extensive use of facial recognition in the UAE can be observed as particularly problematic from a human rights perspective. The UAE has among the highest rates of political prisoners per capita in the world, according to some sources.[517] Coupled with all the other AI and mass surveillance programmes, it provides the government with a multitude of tools for oppression, concealed behind promises of safety, efficiency and convenience.[518]

LAW

The Constitution of the UAE regulates a general right to privacy. Privacy of the home is guaranteed in Article 36, while Article 31 guarantees freedom of communication by post, telegraph or other means of communication and the secrecy thereof, in accordance with the law.[519]

The UAE issued its first federal law to regulate the protection of personal data, the Personal Data Protection Law (PDPL), on 20 September 2021.[520] The PDPL came into force on 2 January 2022, and it will become enforceable six months after the associated executive regulations are issued.[521] These executive regulations are supposed to regulate many of the practical and operational details of the PDPL, but they are still not enacted (despite the fact that PDLP states that this should happen within six months after the date when the law is issued, which expired in March 2022). The UAE Data Office, which will be established under a separate law, will act as the federal data regulator in the UAE.[522]

There are no publicly-available explanations for the delay in the enactment of the executive regulations and the establishment of the UAE Data Office.

Several "free zones", or special economic zones, are located in the United Arab Emirates. Three of these, the Abu Dhabi Global Market (ADGM), the Dubai Healthcare City (DHCC), and the Dubai International Financial Centre (DIFC), have adopted their own data privacy regulations, which are applicable to companies doing business within their jurisdiction.[523]

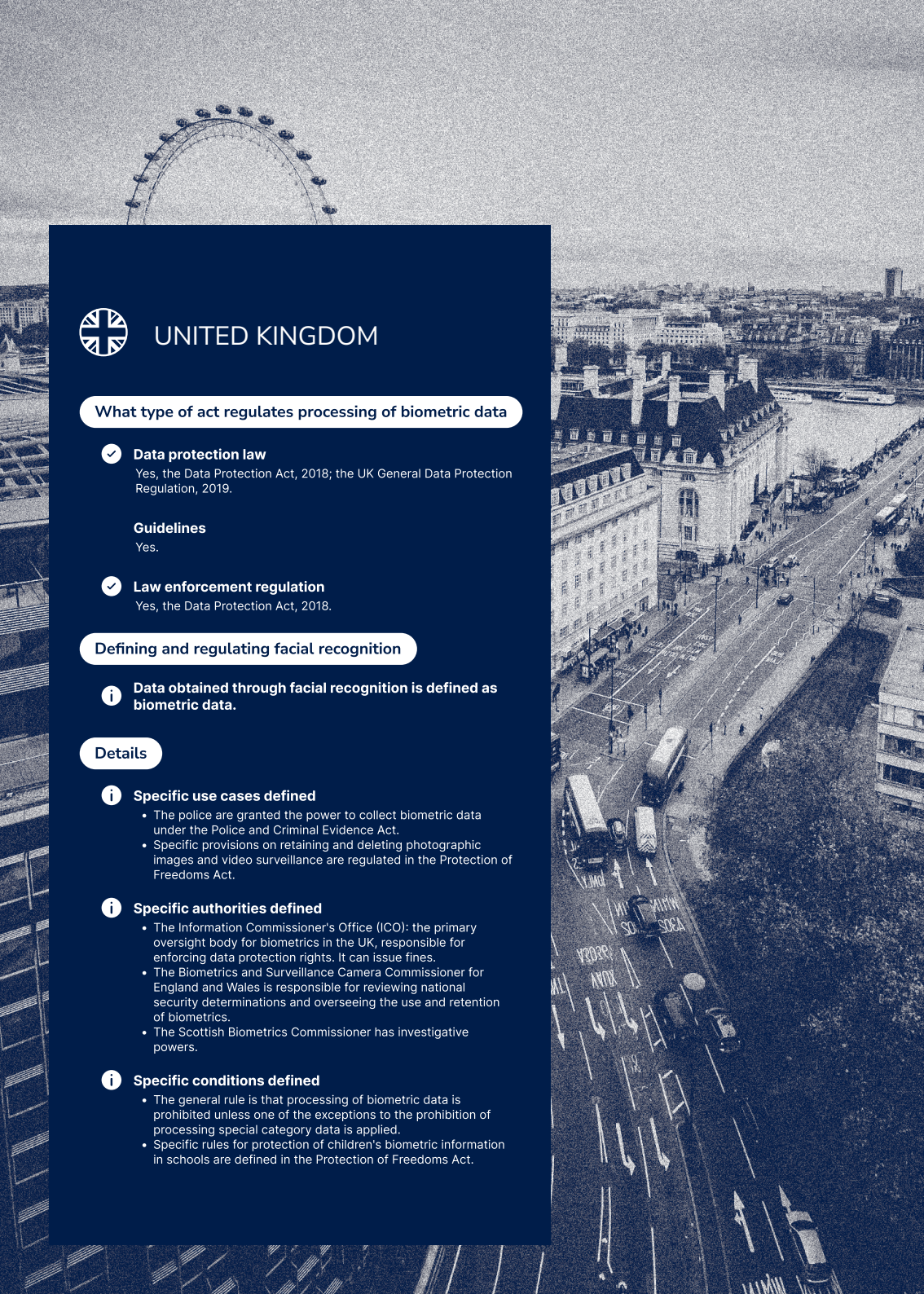
With respect to regulations on facial recognition in the PDPL, the law contains a definition of biometric data that explicitly mentions facial images. The processing of biometric data is not regulated in any specifics but falls within the wider definition of sensitive data (so it is, essentially, a GDPR-style regulatory approach to the matter, same as in Kenya).

There are two main groups of obligations with respect to the processing of any sensitive data: (i) a data protection officer must be appointed when the processing involves a systematic and comprehensive assessment of sensitive personal data, including profiling and automated processing, or processing of large volumes of such data;[524] and (ii) a data protection impact assessment must be prepared before processing that will use any of the modern technologies that would pose a high risk to the privacy and confidentiality of the personal data if the processing will be made on a large amount of sensitive data.[525] No publicly available information indicates that such DPIA has been prepared for use of biometrics for any law enforcement purposes, or that any DPO has been appointed so far.

These DPO and DPIA obligations from PDPL are, therefore, quite similar to those regulated in the GDPR. Notably, however, there are no special conditions or special legal basis that need to be established or met in order for the processing of sensitive data to be allowed, as is required in the GDPR system in the special regime applicable to such data, as regulated in GDPR Article 9. Also, the PDPL does not have the EU Law enforcement directive (LED) type of rules which would govern any specifics when it comes to processing of biometrics, or any other sensitive data, for law enforcement purposes. So, for the time being, it seems that the use of facial recognition by law enforcement agencies happens in a sort of legal vacuum from a data protection regulation standpoint, same as in India and Australia. It remains to be seen whether executive regulations will change this situation.

CASE LAW

There is still no notable case law with respect to the use of facial recognition or other biometric systems in the UAE, relating to the public or the private sector.



UNITED KINGDOM

What type of act regulates processing of biometric data

Data protection law
Yes, the Data Protection Act, 2018; the UK General Data Protection Regulation, 2019.

Guidelines
Yes.

Law enforcement regulation
Yes, the Data Protection Act, 2018.

Defining and regulating facial recognition

Data obtained through facial recognition is defined as biometric data.

Details

Specific use cases defined

- The police are granted the power to collect biometric data under the Police and Criminal Evidence Act.
- Specific provisions on retaining and deleting photographic images and video surveillance are regulated in the Protection of Freedoms Act.

Specific authorities defined

- The Information Commissioner's Office (ICO): the primary oversight body for biometrics in the UK, responsible for enforcing data protection rights. It can issue fines.
- The Biometrics and Surveillance Camera Commissioner for England and Wales is responsible for reviewing national security determinations and overseeing the use and retention of biometrics.
- The Scottish Biometrics Commissioner has investigative powers.

Specific conditions defined

- The general rule is that processing of biometric data is prohibited unless one of the exceptions to the prohibition of processing special category data is applied.
- Specific rules for protection of children's biometric information in schools are defined in the Protection of Freedoms Act.

UNITED KINGDOM

CONTEXT

In 1998, the DNA sample of a man accused of burglary in London was unlawfully retained and later used to identify him in a much more severe case — in which he was convicted of rape and assault.[526] As a result, the law in the UK was changed in 2001 to allow the collection and retention of biometric data almost indefinitely.[527] The UK consequently created the world's largest DNA database, including data from individuals who had not been charged or convicted of crimes, including children.

It was not until a legal challenge in the landmark case at the European Court of Human Rights (ECtHR) of *S. and Marper v United Kingdom* (2008) that legislative changes were made to limit the scope and retention of biometric data under the Protection of Freedoms Act 2012. This new law created the roles of the Biometrics Commissioner, with the main task of reviewing the retention and use of DNA samples, and the Surveillance Camera Commissioner in England and Wales, overseeing compliance with the Surveillance Camera Code of Practice. The proposed Data Protection and Digital Information Bill, set to overhaul the country's post-Brexit data protection regime, suggests abolishing these oversight roles. Experts have expressed concerns over this development, which is seen as weakening oversight, eroding public trust, and overlooking broader surveillance impacts. Critics conclude that removing these functions would further strain an already overburdened and under-resourced surveillance oversight system, reducing their societal value.[528]

One of the most controversial uses of biometric technology in the UK today is the use of live facial recognition (LFR) technology by the police, which gained significant public attention after the

Metropolitan Police Service deployed it at Notting Hill Carnival in 2017[529] and South Wales Police piloted it in 2017-2018. In 2019 and 2020, the Court of Appeal found that the legal framework around the deployment of LFR was insufficient to ensure compliance with human rights.

At the same time, the UK's data protection regulator has raised concerns about technical bias, the effectiveness and the statistical accuracy of LFR systems, and lack of respect for data protection law.[530] In August 2021, over 30 human rights organisations published an open letter calling on the UK Government to completely ban the use of LFR in public.[531]

The use of LFR has so far largely evaded legislative scrutiny by the UK Parliament, with police forces making unilateral decisions on its adoption and safeguards. Despite new guidance and recommendations for proportionality and necessity criteria, privacy assessments, and certain protections of individual privacy rights being implemented since 2018, these recommendations have been ineffective, and concerns over the use of LFR by police persist.[532]

An independent review of UK legislation, commissioned by the Ada Lovelace Institute and led by Matthew Ryder QC, warns that the UK's current legal regime is "fragmented and confusing" and failing to keep pace with developments in biometrics.[533] The review concludes that the country urgently needs new laws to govern the use of biometric technologies and calls for the government to come forward with primary legislation. It also recommends the suspension of LFR in public places until further regulations are introduced.

LAW

The governance of biometric data in the UK is currently regulated by a patchwork of overlapping laws addressing data protection, human rights, discrimination and criminal justice issues. There is no single overarching legal framework for the management of biometric data, and sources of law that developed in response to more general problems regulate biometric data in an ad hoc manner.

Human Rights Act 1998

The Human Rights Act 1998 (HRA) implements many of the rights protected by the European Convention on Human Rights (ECHR) as

part of UK domestic law.[534] It is a relevant legal instrument for regulating biometric data in the UK since it protects the right to privacy in Article 8. Public authorities have to respect an individual's right to privacy under Section 6 of the HRA. However, it does not oblige private companies to uphold human rights, which may be a gap in regulating the use of biometric data by non-public entities.

UK GDPR and DPA 2018

The UK General Data Protection Regulation (UK GDPR)[535] and the Data Protection Act 2018 (DPA 2018)[536] provide the legal framework for the protection of personal data, including biometric data. Along with general provisions, the DPA 2018 implements the Law Enforcement Directive (LED) into UK law, and applies to all the data processing cases involving law enforcement activities. In both UK laws, the definition of biometric data is the same as in the GDPR: "Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

However, it is notable that biometric data have a different definition for the purpose of policing and criminal justice in Scotland, a country in the UK which has devolved powers from England and Wales.[537] This broader definition includes source material (before the specific technical processing), with the aim to protect materials such as fingerprint impressions or facial images, rather than just the resulting biometric templates. This could be seen as a positive application of the ECtHR case *Gaughran v. The United Kingdom* because it recognises the sensitivity of the source photos from which the biometric data are derived. It is also notable with respect to the capabilities of modern surveillance technologies increasing exponentially. This makes it easier and faster to identify and track a person even on the basis of lower-quality data.

The UK GDPR prohibits the processing of special category data, including biometric data, other than in certain limited circumstances. The DPA 2018 complements and customises the conditions for handling special category data under the UK GDPR, allowing the processing for the purposes of employment, social security and social protection, health and social care, public health, archiving, research, and statistics, in relation to criminal convictions or offences, or where there is a substantial public interest,

as long as the specified conditions listed in Schedule 1 are met. Notably, the DPA 2018 adopts a permissive stance, offering up to 23 potential "substantial public interest" conditions that allow for special category data processing. Unlike the Human Rights Act 1998, which applies only to public authorities, Part 2 of the DPA 2018 applies to both public and private sector organisations and individuals when processing data for these purposes.

Part 3 of the DPA 2018 provides for the processing of personal data by competent authorities for criminal law enforcement purposes, including the processing of biometric data to identify an individual uniquely. This kind of processing of biometric data is only lawful if consent has been obtained from the data subject or if it is "strictly necessary", and if it meets at least one of the conditions in Schedule 8 of the DPA 2018.

Part 4 of the DPA 2018 concerns data processing by UK intelligence services, defined as MI5, MI6 and GCHQ. Usage of biometric data for identifying individuals is categorised as sensitive processing and can only be done if certain conditions in Schedule 9 and Schedule 10 are met.

The Information Commissioner's Office (ICO) is the primary oversight body for biometrics in the UK, as it is responsible for enforcing data protection and freedom of information rights. The ICO has so far issued two opinions on facial recognition technology, focusing on law enforcement use,[538] and the use of biometric technology for identification and categorisation in public places.[539]

PACE and anti-terrorism acts

Police and other law enforcement authorities in the UK have specific powers to collect and retain biometric data for criminal justice and anti-terrorism purposes. These powers are granted through various legislations, including the Police and Criminal Evidence Act 1984 (PACE),[540] the Terrorism Act 2000,[541] the Counter-Terrorism Act 2008, the Terrorism Prevention and Investigation Measures Act 2011, and the Counter-Terrorism and Border Security Act 2019.

Under PACE, the police have the power to take fingerprints, "intimate and non-intimate" (DNA) samples, and photographs of suspects subject to a criminal investigation. Section 63D of PACE requires fingerprints and DNA profiles derived from DNA samples to be destroyed if it appears they

were taken unlawfully, or based on an unlawful arrest or an arrest premised on mistaken identity.

The Terrorism Act 2000 grants police the power to stop, question and detain individuals at ports or border areas to determine if they are involved in acts of terrorism, and authorises the collection of biometric data in certain circumstances. Schedule 8 outlines the circumstances under which fingerprints and non-intimate DNA samples can be taken, including without consent if authorised by a superintendent. Schedule 8 sets up a general retention period of 6 months at maximum, unless a national security determination authorises their retention for a longer period. Similar provisions for biometric data retention also appear in other legislation related to counter-terrorism measures.

PoFA

The Protection of Freedoms Act 2012 (PoFA)[542] was partly enacted as a reaction to the ECtHR decision in the *S. and Marper* case, which found that the UK's collection and retention of biometric data violated Article 8 of the ECHR. The PoFA regulates the processing of biometric data by public and private actors, and includes provisions for retaining and deleting DNA, fingerprints, photographic images and video surveillance. The PoFA also inserted provisions for retaining and deleting biometric data in the Police and Criminal Evidence Act 1984 (PACE) and established the Biometrics Commissioner and Surveillance Camera Commissioner, responsible for making national security determinations and keeping under review the use and retention of biometrics.

Additionally, Chapter 2 of Part 1 of the PoFA provides for the specific protection of children's biometric information in schools, requiring parental consent and providing alternative means for children who object to the processing of their biometric information. If a child objects to their biometric information being processed, even if the parent consents, the school must provide reasonable alternative means for the child to participate in activities.

The Biometrics Commissioner's role, established under the PoFA, is independent of the government and has limited scope in reviewing the use of biometric data. The Commissioner's four specific functions include:

» reviewing the retention and use of DNA samples;

- determining applications to retain DNA profiles and fingerprints;
- reviewing national security determinations; and
- providing reports to the Home Secretary (the UK's Interior Minister).

Although the scope is limited, the Commissioner can address topics beyond its immediate scope due to the power to report on any matter relating to its functions.

The Surveillance Camera Commissioner has three primary functions:

- encouraging compliance with the Surveillance Camera Code of Practice;
- reviewing the operation of the Code; and
- providing advice to the government regarding changes or breaches of the Code.

The definition of "surveillance camera systems" used by the Surveillance Camera Commissioner includes CCTV and any system associated with it or connected to it, including vision-based biometrics. Although the Commissioner does not have enforcement functions or powers of inspection, it provides advice on the effective and appropriate use of surveillance camera systems, including biometric technologies, which must be justified, proportionate, and for a stated purpose. The updated Code of Practice provides guidance on the use of live facial recognition technology by chief officers of police, including establishing an authorisation process and criteria for deployment.

The roles of the Biometrics Commissioner and Surveillance Camera Commissioner for England and Wales were merged into a single appointment in March 2021, prompting criticism from the previous post-holders.[543] No new law has been introduced to define the new role, and the legal basis is expected to remain the same. The government suggested in September 2021 that the functions of the Commissioner's role could be integrated into the ICO, a move which as of 2023 seems to be in motion.

Notably, the situation in Scotland is different from England and Wales, and the Scottish Biometrics Commissioner (SBC) was appointed in 2020

through the Scottish Biometrics Commissioner Act.[544] In 2022, the SBC brought in a binding Code of Practice for the processing of biometric data by police.[545] When it comes to oversight of the police, the SBC also possesses investigatory powers. As explored here and later in the Practice section, the police use of live facial recognition in public spaces has been prolific in England and Wales, whereas to date, these systems have never been deployed in Scotland.

CASE LAW

As mentioned, the ECtHR decision of *S. and Marper v United Kingdom* (2008)[546] had a crucial role in interpreting the impact of biometric data processing on human rights. The ECtHR concluded that the collection of biometric data about a person "allowing his or her identification with precision in a wide range of circumstances" is "capable of affecting his or her private life" and gives rise "to important private-life concerns".

In addition, for the collection and retention of biometric data to be lawful, the Court found that it is essential to have "clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness".

The case of *R (Bridges) v Chief Constable of South Wales Police* (2020) dealt with the police use of automatic live facial recognition (LFR) technology on crowds.[547] The Court of Appeal found that the use of LFR by the police was unlawful as it breached privacy rights, data protection laws, and equality legislation. It also held that South Wales Police piloting of LFR had not satisfied the "in accordance with law" requirement and, as such, violated Article 8 of the ECHR since the legal framework was insufficient to protect individual rights. The High Court pointed out that Article 8 is engaged whenever biometric data are captured, stored or processed, even momentarily.

If a measure interferes with Article 8 of the ECHR and is in accordance with the law, the next step is to consider whether it is necessary and proportionate in a democratic society. That requires identifying a legitimate aim, assessing whether the interference is proportionate to achieving that aim, and that the means that will be pursued are effective. Proportionality is assessed by a

four-stage test established by the UK Supreme Court in *Bank Mellat v HM Treasury* (No 2) (2013).[548]

The four stages of the test are: (1) whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right; (2) whether it is rationally connected to the legitimate aim; (3) whether a less intrusive measure could have been adopted without unacceptably compromising the objective; and (4) whether a fair balance has been struck between the rights of the individual and the interests of the community, taking into account the severity of the consequences.

UNITED STATES

What type of act regulates processing of biometric data

Special law on biometric data
Yes.

Law enforcement regulation
Generally no; aspects of law enforcement powers are regulated by a special law on biometric data.

Criminal Law
Generally no; some aspects of criminal law are regulated by a special law on biometric data.

Local level legislation
Yes; applicable at the state and municipal levels.

Defining and regulating facial recognition

Facial recognition is explicitly defined in many states.

Details

Specific use cases defined

- Most laws regulate FRT use by law enforcement or, more generally, by public authorities.
- Most laws explicitly regulate when FRT use is allowed and/or it is not allowed (some laws provide list of such cases).
- Some laws specifically address real-time FRT use and regulate when it is permitted.
- Some laws regulate use of facial recognition in the context of criminal law, limiting the types of offences that can be investigated using FRT.
- Some laws regulate specific uses such as searching for missing or deceased persons.

Specific authorities defined

- Different dedicated authorities have varying powers, but mainly, they involve either ex ante (prior) or ex post (after the fact) supervision.
- No dedicated authority has the power to halt the use or impose fines for illegal use.

Specific conditions defined

- Most common conditions for the use of facial recognition include testing, training, reporting obligations to specific authorities, and transparency to the public.
- Some laws stipulate a need for human involvement to verify search results.

UNITED STATES

CONTEXT

The use of facial recognition technology (FRT) in particular — as opposed to other types of biometric surveillance — is very present in the United States, and has been highlighted in several FRT monitoring projects,[549] and reports,[550] due to how prolific its use is.

Despite this, regulation on FRT in the US is currently a patchwork of laws that regulate different aspects of the technology at state or other local levels, including municipalities. These laws are very different from one another in terms of what they regulate: some address commercial use, others tackle law enforcement use or even more specific situations such as use in schools,[551] in the workplace,[552] or exceptions for purportedly tackling child sexual abuse and human trafficking.[553]

Notably, there is no law on the federal level that regulates the use of FRT. This gap has been recognised, and there have been several initiatives and proposals on how Congress should approach this matter, but as of yet, with no resolution.[554]

A moratorium, which would effectively ban the use of facial recognition by law enforcement in the US for a set time period, has been proposed on several occasions,[555] most recently in 2023 in the form of the "Facial Recognition and Biometric Technology Moratorium Act of 2023".[556] According to this proposal, a prohibition on the use of FRT by federal entities can only be lifted with an act of Congress. The bill should regulate the use of other biometric data as well, such as voice and gait recognition. The enactment of this bill would not, however, prevent the states and localities from enacting their own laws that more strictly regulate the use of facial recognition and other biometric technologies.[557]

One of the proposals on how to set limits on, instead of fully prohibit, FTR came up in 2022 in the form of a draft "Facial Recognition Act".[558] The idea of this proposal is to set up a regulatory regime for state and federal law enforcement use of FRT, both in cases when there are risks because FRT doesn't work well, and in cases when it works as intended, but enables uses by law enforcement which would unacceptably limit human rights.[559] The proposed legislation would prevent law enforcement officials from utilising face recognition software in ways that could amount to mass surveillance, including utilising the technology in conjunction with dashboard and body cameras, as well as when there are public demonstrations.[560]

Based on the experiences at state level, there have been proposals for which elements of FRT should be regulated on a federal level, such as implementing: (i) a court warrant requirement based on probable cause; (ii) a serious crime requirement; (iii) transparency of use; (iv) safeguards so that FRT cannot be the sole basis for an arrest; (v) the prohibition of untargeted scans where the system identifies all individuals in a video feed; and (vi) setting up testing and accuracy standards.[561]

LAWS

Overview of the US legal landscape

According to the taxonomy of approaches for regulating FTR in the US proposed by the AI Now Institute, there are three general legislative options: (i) complete bans; (ii) moratoria that can be further broken down into two types: time-bound moratoria, which "pause" the use of FRT for a set amount of time, and directive moratoria, which "pause" until legislative action is taken that will supersede the moratoria; and (iii) regulatory bills which create parameters.[562]

Complete bans and moratoria on the state or private use or both have mostly been introduced by municipal governments,[563] or proposed on state and other local levels.[564] Some states have introduced moratoria that were replaced by subsequent regulation, as was the case in Virginia in 2022,[565] and Vermont in 2021 (where the complete ban was somewhat relaxed for strictly limited exceptions), which are elaborated in more detail later in this section.[566] In California, for example, the 2019 moratorium simply expired (without a replacement law being passed, although some proposals were on the table).[567] The situation is similar in New Orleans, where the moratorium

was dropped over a period of two years.[568] The reasoning behind this change of heart was presumed to be an increase in violent crimes,[569] and an increase in industry lobbying.[570]

The regulation of the use of facial recognition and other biometric systems for both commercial and private purposes was pioneered by the state of Illinois, which passed the Biometric Information Privacy Act (BIPA) in 2008.[571] BIPA regulates the collection of biometric data and limits private companies' right to collect such data without consent. It also creates a right of action (the right, here for an individual, to take legal action against someone in a court of law) and a right to compensation for damages from offending companies. In 2009, Texas passed a similar law,[572] except it lacked the right for individuals to sue, i.e. claims for violations can only be filed by the state. Similar laws have been enacted in the state of Washington, the city of Portland and New York City.[573]

When it comes to the specifics of the legal provisions that regulate facial recognition — as well as occasionally other forms of biometric surveillance — for law enforcement purposes, several overlapping options have emerged in the US. A comprehensive overview by the Center for International and Strategic Studies (CSIS) of the enacted laws and available legislative proposals, at federal state and other local levels, identifies a number of legal options to address different phases of the development and deployment of systems, as summed up below.[574]

Some US laws regulate the phase before the technology is implemented, by asking for the authorisation and/or oversight of the deployment of facial recognition systems by governments. For example, in some states, there is a requirement to seek permission from a legislative body before law enforcement agencies can purchase and install facial recognition systems (as seen in both Washington and Colorado via a mandatory notice of intent). In some other states, there are mandatory steps before the technology can be used by law enforcement agencies in a concrete case, such as: (i) instituting oversight through authorisation for a small number of organisations to use facial recognition (in Massachusetts and Utah, police must submit written requests to state agencies, which then determine whether to conduct the search on their behalf); and (ii) imposing judicial oversight by requiring law enforcement agencies to obtain a warrant or a court order before using facial recognition (Washington, Colorado and Massachusetts).

Circumstances under which FRT can and cannot be used vary significantly. Some laws include lists of cases when FRT use is allowed, thereby excluding all other situations from permissible use (such as Vermont), and usually include crime-related and investigative uses, sometimes limited to only certain crimes (as in Utah), or specifically for the search for missing or deceased persons (Washington, Colorado, Maine, Virginia, Utah and Massachusetts). Other laws specifically prohibit certain uses, such as searches made on the basis of an individual's religion, race, gender, political affiliation, or any other characteristics protected by law (Washington and Colorado); and/or positive matches being used to establish probable cause in a criminal investigation, in the absence of other forms of evidence (Washington, Colorado, Maine, Virginia and Alabama); or the creation of a record describing an individual's exercise of rights guaranteed by the First Amendment (that protects freedom of speech, the press, assembly, and the right to petition the Government for a redress of grievances), although the exact content of this prohibition remains to be seen in time (Washington and Colorado).[575]

Requirements for transparency come in various forms. Some laws require that already in the procurement procedure some features of the technology that is to be purchased are established (an accountability report must be prepared in Washington and Colorado prior to developing, procuring, or using a facial recognition system or service). Some laws regulate that the public — i.e. people affected — must be properly notified before the technology is deployed (Utah), or that notice must be given to defendants if facial recognition was used to assist in an investigation (Washington and Colorado). Many states also have requirements that, after facial recognition technology has been deployed, the details and results of its use are made available to the public in the form of different reports (whose content is also regulated).

Technology testing requirements may include (i) the obligation to test the technology in operating conditions before it is used; and (ii) ongoing testing to check performance differences and enable the mitigation of any "unfair" performance discrepancies across various "subpopulations" (Washington and Colorado). Similarly, (iii) to mitigate the risk of mistakes and misidentification, some laws require human intervention to verify a positive match in certain situations (Washington, Colorado and Utah). Some laws also (iv) regulate training obligations for persons (i.e. employees)

who are actually operating the technology (Washington, Colorado, Utah, Virginia and Kentucky).

Finally, some laws explicitly make a distinction between ongoing or real-time surveillance (Washington, Colorado and Virginia), and treat it more restrictively than subsequent retrospective surveillance (for example the analysis of CCTV feeds), while in many states only the latter is permitted.

There are also other ways of categorising these different legislative approaches. The University of Pennsylvania differentiates between the laws that: (i) limit the circumstances in which facial recognition can be used; (ii) evaluate the technology against predefined principles or guidelines for appropriate usage; (iii) ensure public engagement and approval as a prerequisite to the deployment of the technology; and (iv) stipulate comprehensive requirements that combine aspects of the aforementioned three approaches.[576]

The following sections provide an overview of legal provisions regulating facial recognition technology throughout the US at the time of writing, followed by a description of the particular state laws.

Summary of legal provisions at the states level

Legal provisions regulating FRT use by law enforcement agencies from different state laws can be classified based on several criteria, including their popularity (from those that are most common to those that are somewhat "exotic") or phase of the FRT use that they regulate. The summary that follows is a non-exhaustible list of legal solutions present in the US to date taking in particular these two criteria into account.

Legal regime only for law enforcement or also for other state authorities

Some states have laws that specifically target law enforcement agencies with their facial recognition regulations. These are Virginia, Alabama, Massachusetts, Vermont and Kentucky. Other states aim to have rules that regulate how FRT can and cannot be used by other state authorities as well.

In Washington and Colorado, the law applies to state and local government agencies. In Maine, it applies to state, county or municipal government or a department, agency or subdivision thereof, or any other entity identified in law as a public instrumentality, including, but not limited to, a law enforcement agency and its public employees or officials. In Utah, the law

is directed at government entities, while the list of the exact such entities is specified in the text of the law.

Legal regimes that have a general ban subject to exceptions, allow for specific uses, or explicitly ban some uses

Laws in the US vary in terms of how they generally approach FRT regulation. Most laws start with the general ban on FRT use and then allow for some exceptions. Others do not spell out the ban or prohibition but do regulate circumstances or situations when the technology can be used.

It might be interpreted that this distinction is only a variation in the wording used and that the end result is the same — FRT use is legal only in the presence of the exception, situation or circumstances specified in the law.

However, it can also be argued that this is not only a semantics issue, but that the chosen approach can have some legal consequences. One of the general rules or guidance that lawyers use in order to interpret the law is that exceptions are to be interpreted narrowly, commonly referred to with the Latin phrase "*expressio unius esclusio alterius*". The application of this interpretative tool could effectively narrow down the permissible use cases for facial recognition in the states that took the "exceptions" approach. On the other hand, there is interpretative guidance according to which a provision may apply by analogy to a situation that is similar to the one spelt out in that legal provision, but not expressly mentioned. This rule, "*ejusdem generis*" in Latin (or "of the same kind"), may be used to broaden the scenarios in which permissible uses are applicable, i.e. it can widen the application of the FRT in the states that took the latter approach.

Vermont, Alabama, Utah and Maine took the first approach, while Massachusetts assumed the second one.

Some states have provisions that explicitly ban certain FRT uses, in order to make sure that no interpretation tools can be used to legalise them. Such provisions are to be found in the laws of Washington, Colorado, Virginia and Utah.

Real-time surveillance

Some laws explicitly regulate the use of facial recognition tools in real-time, or other similar scenarios. These rules, therefore, directly tackle mass

biometric surveillance scenarios via use of facial recognition tools. The states that have some legal rules on this, mostly forbid real-time or near real-time surveillance or exceptionally allow it under some very limited conditions.

Colorado law defines "ongoing surveillance" as the continual use of a facial recognition service by an agency to track in real-time the physical movements of a specified individual through one or more public places. However, this definition does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time after the individual has been recognised. "Persistent tracking" is defined as the use of FRT by an agency to track the movements of an individual on a persistent basis without identification or verification of the individual. The tracking becomes persistent as soon as (i) the facial template that permits the tracking is maintained for more than forty-eight hours after first enrolling that template; or (ii) data created by the facial recognition service is linked to any other data such that the individual who has been tracked is identified or identifiable.

The law continues by regulating that the law enforcement agency shall not use a facial recognition service to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless: (i) the agency obtains a warrant authorising such use; (ii) such use is necessary to develop leads in an investigation; (iii) the agency has established probable cause for such use; or (iv) the agency obtains a court order authorising the use of the service for the sole purpose of locating or identifying a missing person or identifying a deceased person.

Washington law has the same definition of "persistent tracking" and a similar definition of "ongoing surveillance", with one addition. Namely, it specifies that an ongoing surveillance includes the use of FRT in real-time, but also through the application of a facial recognition service to historical records. Regulation of situations when ongoing surveillance, real-time or near real-time identification, or persistent tracking would be allowed are also somewhat different when compared to Colorado laws, and include situations when (i) a warrant is obtained authorising the use of the service for those purposes; (ii) exigent circumstances exist; or (iii) a court order is obtained authorising the use of the service for the sole purpose of locating or identifying a missing person, or identifying a deceased person.

According to the laws in Virginia, the law enforcement agency is not allowed to (i) use FRT for tracking the movements of an identified individual in a

public space in real time; or (ii) create a database of images using a live video feed to use FRT.

Evaluation of the technology before it is used

Both Washington and Colorado laws regulate the procedure to be undertaken before any facial recognition service is put in use, which is twofold: (i) notice of intent must be submitted to the competent body, and then (ii) an accountability report must be prepared and made public. The content of the accountability report is regulated in detail in the text of both laws and includes, *inter alia*, technical specifications, management policy, testing procedure, rate of false matches, and description of impact of the facial recognition use on civil rights and liberties. Before the accountability report is adopted, it has to be available for public debate.

In Virginia, the law regulates that any facial recognition technology in use shall utilise algorithms that have demonstrated (i) an accuracy score of at least 98% true positives within one or more datasets, and (ii) minimal performance variations across demographics associated with race, skin tone, ethnicity or gender. This test is to be performed by the National Institute of Standards and Technology as part of the Face Recognition Vendor Test before the technology is purchased. In addition, any local law-enforcement agency must have in place a policy regarding the use of facial recognition technology before employing such technology to investigate a specific criminal incident or citizen welfare situation, or it may adopt the State Police Model Facial Recognition Technology Policy (if the agency opts to develop their own policy, it must meet or exceed the standards set forth in such state model policy). The agency must publicly post and annually update its policy.

When compared to the GDPR rules, these provisions seem to be following the same logic as a requirement that DPIA must be prepared before deployment of the technology that might result in a risk for the rights and freedoms of natural persons.

Transparency after the technology is used

In the phase after the technology is used for some time, several laws regulate that there must be a level of transparency that would enable public accountability. Such transparency provisions are mostly to be found as the requirement for reports to contain some statistical information. Therefore,

this is somewhat different to GDPR-like regimes, where transparency is primarily to be achieved via privacy policies and similar documents (that must contain all the information in line with Articles 12 and 13 of the GDPR).

In Washington and Colorado, appropriate records must be kept by the authorities that have used the technology, but also by judges who issued or extended warrants for the use of the technology, or denied the approval for such warrants. Both also have to provide annual reports, whose contents are regulated in the law.

In Virginia, any agency that uses facial recognition technology must publicly post and annually update a report to provide information to the public regarding the agency's use of FRT. The minimum content of the report is regulated by the law. The agency must also publicly post and annually update its policy regarding the use of facial recognition technology.

In Utah, government entities must release statistical information regarding facial recognition comparisons, upon request. Such statistical information may include (i) the different types of crime for which the government entity received a request; (ii) how many requests the government entity received for each type of crime; and (iii) the number of probable matches the government entity provided in response to each request. The entity must also prepare annual interim reports to the government's competent committee. In addition to statistical information from points (i) to (iii), the report must also include the image source from which the department made each match. The law explicitly regulates that in responding to a request for a release of statistical information or preparing the respective report, a government entity may not disclose details regarding a pending investigation.

The law in Maine regulates that the authorities performing searches must maintain logs that track all requests for searches of facial surveillance systems received and performed by them. De-identified logs containing the date of the search request, the name of the public employee or public official who made the request and the name of the department for which the employee or official works, the databases searched, the statutory offence under investigation and the race and sex of the person under investigation are public records for the purpose of state regulations that regulate freedom of access to public information.

Pursuant to the law in Massachusetts, agencies must document (again, in content regulated by the law) each facial recognition search performed, and provide such documentation quarterly to the executive office of public safety and security. This office has the obligation to annually publish on its website documentation received from law enforcement agencies, as well as additional data for the previous calendar year with total numbers from the whole state (as is also regulated in law in detail).

Ongoing testing

Several states have rules that aim to make sure that the conditions the technology must fulfil are met not only before the technology is purchased or put into function, but also throughout its life cycle. These types of provisions are not so common outside the USA.

Washington and Colorado laws have the most elaborated rules on how the technology must be tested for accuracy and bias control. Prior to deploying FRT that will be used for making decisions that produce legal effects on individuals or similarly significant effects, such service must be tested in operational conditions. Furthermore, an agency must require a service provider to make available an application programming interface or other technical capabilities to enable legitimate, independent, and reasonable tests for accuracy and unfair performance differences across distinct subpopulations (such subpopulations being defined by visually detectable characteristics such as race, skin tone, ethnicity, gender, age, etc.). If the results of the independent testing identify material unfair performance, the provider must develop and implement a plan to mitigate the identified differences.

In Virginia, an annual test must be done to verify that the conditions for deployment of the technology are still satisfied, i.e. according to the law, all approved vendors must annually provide independent assessments and benchmarks offered by the National Institute of Standards and Technology to confirm continued compliance with the legal requirements..

Training of personnel

Another US-specific type of legal requirement is, again, aimed at making sure that the technology is used in a legal manner. Not only must the technology satisfy predefined conditions and be tested regularly, but the

people who work with that technology must be knowledgeable about how to properly use it.

The training of officers or officials who will use FRT in practice is regulated in detail in Washington and Colorado laws, including the training requirements. These should cover as a minimum: (i) the capabilities and limitations of the FRT; (ii) procedures to interpret and act on the output of the FRT; and (iii) to the extent applicable to the deployment context, the meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects.

Other laws do not go into so much detail. Pursuant to the law in Virginia, the Department of State Police must develop and publish a State Police Model Facial Recognition Technology Policy. This model policy must, inter alia, include requirements for training facilitated through the department, covering the nature and frequency of specialised training required for an individual to be authorised by a law enforcement agency to utilise FRT.

Similarly, the law in Kentucky regulates that a model policy will be developed by an appointed working group, and such policy will specify training procedures and processes to ensure all personnel who utilise FRT or access its data are knowledgeable about and able to ensure compliance with the policy.

Probable cause in a criminal investigation

This requirement is to be interpreted in accordance with US criminal law provisions. However, since facial recognition in the context of law enforcement use is, to a large extent, directly related to investigations and criminal procedures, similar legal provisions can be found in other legal systems as well. For example, in India, the Delhi police relied on Indian criminal law as an alleged legal basis for their use of FRT (although Indian criminal law does not spell out any rules on the significance of facial recognition-related evidence in criminal procedures).

Several US states regulate prohibition on the use of positive matches from FRT to establish probable cause in a criminal investigation, with some local differences. In Alabama, the law adds a rule that a state or local law enforcement agency may not use match results to make an arrest.

Alabama, Washington and Colorado laws regulate that the results of a facial recognition service may be used in conjunction with other information and

evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation (or also to make an arrest in Alabama).

According to the law in Virginia, a match made through FRT shall not be included in an affidavit to establish probable cause to issue a search warrant or an arrest warrant, but shall be admissible as exculpatory evidence.

According to the law in Maine, facial surveillance data does not, without other evidence, establish probable cause justifying arrest, search or seizure.

Limited scope of crimes

The use of FRT by law enforcement agencies is generally directed to the investigation of crimes. While most of the US laws do not differentiate between crimes in terms of permissible uses, some states have limited such uses of facial recognition tools to more serious crimes.

Maine law contains a definition of a serious crime and limits the permitted purpose for facial recognition uses to investigate such serious crimes when there is probable cause to believe that an unidentified individual in an image has committed it. "Serious crime" is defined as any crime punishable by a term of imprisonment of one year or more and some specific crimes regulated in their Statutes — if the law of Maine applies to legal qualification. If the criminal laws of another jurisdiction are applicable, serious crime is defined as a crime that involves the use of a firearm or other dangerous weapon against a person or is punishable by a term of imprisonment of one year or more.

The law in Utah limits uses to investigations of a felony or a violent crime or, more generally, a threat to human life.

When it comes to situations in other worldwide jurisdictions, the first and second draft of the legal provisions in Serbian draft laws that would regulate FRT use by the police included all the crimes that are to be prosecuted by the state, i.e. crimes procedure based on private claims were not covered. However, the latter category includes very few crimes, such as those against dignity and intellectual property rights, or some minor crimes like slight physical injuries or petty theft.

Identification of a deceased and/or missing person

Laws in Washington and Colorado have the same provision on this topic — the law enforcement agency can use a facial recognition service if it obtains a court order authorising the use of the service for the sole purpose of locating or identifying a missing person or identifying a deceased person.

The definition of an "authorised use" of FRT in the law of Virginia includes the identification of a deceased or missing person. Similarly, the law in Maine allows for the use of FRT by government entities if the purpose is assisting in the identification of a person who is deceased or believed to be deceased, as well as of a missing person.

Two states excluded the identification of a missing person as a permissible use case. In Utah, the use of FRT is allowed for the purpose of identifying an individual who is deceased, incapacitated, or at risk and otherwise unable to provide the law enforcement agency with his or her identity. The law in Massachusetts regulates that a law enforcement agency can use FRT without a court order in order to identify a deceased person.

Requirement for human intervention

While some laws take into account that humans may make errors, and thus require that persons who use technology in practice must be properly trained to do so, other laws take into account that the technology will make errors as well.

Laws in Washington and Colorado regulate situations when humans must verify positive matches. According to laws in both of these states, an agency using FRT to make decisions that produce legal effects concerning individuals, or similarly significant effects on individuals, must ensure that those decisions are subject to meaningful human review. "Meaningful human review" is defined as a review or oversight by one or more trained individuals who have the authority to alter the decision under review.

According to the law in Utah, if the facial recognition system indicates a possible match, an authorised employee must make an independent visual comparison of such a match. The law details further procedure depending on whether such visual comparison shows that the match is just possible or probable. Probable matches must go through a second round of human comparison, and this second opinion is to be given by another trained

employee or a competent supervisor. Thus, the final decision about whether to treat the match as probable is always to be made by a human.

Authorisation to run the search

Some states have adopted a rule according to which police officers cannot have direct access to FRT to run comparisons, but must require another authority to do so. This is a sort of safeguard against the unauthorised use or misuse of the technology by the police.

In Maine, the requests for searches of facial surveillance systems go through the Bureau of Motor Vehicles, except in some narrow and specific situations.

In Massachusetts, any law enforcement agency performing or requesting a facial recognition search using FRT shall only do so through a written request submitted to the registrar of motor vehicles, the Department of State Police, or the Federal Bureau of Investigation.

In Utah, a law enforcement agency should submit a request for a facial recognition comparison on an image database to the government entity that manages the respective database, or the Department of Public Safety if the database in question is shared with or maintained by that department.

Penalties for officers who violate the law

Some states prescribe penalties for officers or other persons who use the technology in violation of the law. This approach could probably be related to the general legal regime in those states, where implementation of this provision has some track record in practice in similar scenarios. Even though this seems like a powerful legal tool to deter a person from acting contrary to their legal obligations and duties, it is unlikely to be followed in legal systems (like in some civil law countries) that do not generally take this approach to secure the accountability of public officials.

The law of Virginia imposes such a penalty for any operator employed by a local law enforcement agency who (i) violates the agency's policy for the use of FRT or (ii) conducts a search for any reason other than an authorised use. Such an operator is guilty of a misdemeanour and shall be required to complete training on the agency's policy on authorised uses of technology before being reinstated to operate such FRT. The local law enforcement agency shall terminate from employment any FRT operator who violates

clause (i) or (ii) for a second time. An operator who commits a second or subsequent violation is also guilty of a more serious misdemeanour.

According to the law that regulates the use of facial recognition in Maine, a public employee or public official who, in the performance of their official duties, violates the provision of the law may be subject to disciplinary action, including, but not limited to, retraining, suspension or termination, subject to the requirements of due process and any applicable collective bargaining agreement.

Moratorium until there are relevant regulations in place

Vermont and Kentucky have passed laws which effectively put a moratorium on the use of FRT by law enforcement agencies until there are relevant legal rules in place for such use.

In Vermont, rules must be passed by the General Assembly of Vermont.

In Kentucky, a working group on facial recognition technology was established with a mandate to create a policy specifying rules on the use of FRT by law enforcement agencies. The law sets a deadline for producing such a policy by 1 January 2024.

Exception for criminal investigation into the sexual exploitation of children

Vermont law bans all facial recognition uses for the time being, but does provide for one exception: enforcement purposes during a criminal investigation into the sexual exploitation of children.

	WASHINGTON	COLORADO	VIRGINIA	MAINE	UTAH	MASSACHUSETTS	ALABAMA	VERMONT	KENTUCKY
Legal regime only for law enforcement agencies			✓			✓	✓	✓	✓
Legal regimes that have a general ban on FRT use, subject to exceptions				✓	✓		✓	✓	
Legal regimes that allow FRT use for specific purposes						✓			
Explicit ban on certain FRT uses	✓	✓	✓		✓				
Regulation of real-time surveillance	✓	✓	✓						
Evaluation of the technology before it is used	✓	✓	✓						
Transparency after the technology is used	✓	✓	✓	✓	✓	✓			
Ongoing testing	✓	✓	✓						
Training of personnel	✓	✓	✓						✓
Prohibition to establish probable cause in a criminal investigation	✓	✓	✓	✓			✓		
Limited scope of crimes				✓	✓				
Identification of deceased person	✓	✓	✓	✓	✓	✓			
Search for missing person	✓	✓	✓	✓					
Requirement for human intervention	✓	✓			✓				
Authorisation to run the search				✓	✓	✓			
Penalties for officers who violate the law			✓	✓					
Moratorium until there are relevant regulations in place								✓	✓
Exception for a criminal investigation into the sexual exploitation of children								✓	

State of Washington

In March 2020, the state of Washington passed a comprehensive bill that regulates the use of facial recognition by all government entities, state and local, including law enforcement (with an effective date of 1 July 2021).[577] Some commentators described the bill as an attempt to find a compromise between an outright ban on FRT and its indiscriminate use.[578] The aim of introducing the bill was two-fold: to create a legal framework by which FRT can be used to the purported benefit of society, while protecting society from uses that threaten democratic freedoms and put civil liberties at risk.[579]

The American Civil Liberties Union (ACLU) voiced concerns that the bill's safeguards were too weak, and that the law lacks "meaningful accountability or enforcement measures". It was further criticised for allowing the use of FRT when making government decisions regarding financial and lending services, housing, insurance, education, criminal justice, employment, health care and basic necessities as long as those decisions undergo a loosely-defined "meaningful human review".[580]

Since the bill was sponsored by a senator who at the time worked as a senior programme manager at Microsoft, there has been speculation regarding Microsoft's undue influence in the legislative process.[581]

The bill regulates different aspects of FRT deployment, including imposing obligations before the deployment of technology, as well as some transparency and accountability mechanisms. Based on the text of the law, these rules can be summed up as follows:[582]

- **Notice of intent and accountability reports —** The bill creates an obligation for any agency wanting to use FRT to file a notice of intent with the appropriate legislative authorities before deploying the technology. The agency must also create a public "accountability report" which would provide details about a number of points listed in the bill (the agency can commence working on the accountability report once it files the notice of intent by the legislative authority). Before the facial recognition system is implemented, the report will be open to public review and comments, and has to be updated when required.
- **Human review and testing —** Agencies that use FRT to make decisions that produce legal effects concerning individuals

must test it in operational conditions and must also ensure those decisions are subject to "meaningful" human review — although this term is poorly defined, raising questions about how meaningful this review would actually be.

» **Performance discrepancies —** To enable independent testing for accuracy and to ensure that there are not "unfair" performance discrepancies across various "subpopulations", agencies must mandate that a service provider make an application programming interface (API) available. If the independent testing uncovers unfair performance discrepancies between subpopulations, the provider must create and carry out a plan to correct them. However, as discussed at length in the Practice section, such a narrow focus on technical bias can obfuscate broader harms, especially at the societal level, such as systemic racism. This is especially the case here, where surveillance uses are still permitted, despite the systemic risks that they pose to rights including privacy, equality and non-discrimination.

» **Training —** Employees who work with FRT must receive regular training. Minimum training requirements are specified in the bill.

» **Record-keeping —** Any agency using FRT must maintain records that are sufficient to facilitate public reporting and auditing of compliance.

» **Criminal law and judiciary —** Agencies are obliged to proactively inform a defendant before trial when facial recognition has been used in their case. Agencies and judges involved in granting, extending or denying warrants for FRT must provide annual reports with at least the information regulated in the bill.

» **Use for surveillance, including real-time identification and persistent tracking —** Agencies are allowed to use FRT for ongoing surveillance, real-time or near-real-time identification, and persistent tracking (defined in the bill as tracking an individual's movements without identifying that individual) only in three scenarios: (i) with a warrant; (ii) if there are exigent circumstances; or (iii) with a court order for the sole purpose of locating or identifying a missing or deceased person.

- **Prohibitions —** The bill prohibits several uses explicitly, such as (i) applying facial recognition based on religious or political views, gender, gender identity, actual or perceived race, ethnicity, citizenship, age, or disability (while the bill explicitly regulates that this prohibition does not condone profiling including, but not limited to, predictive law enforcement tools). FRT may also not be used: (ii) to identify an individual based on a sketch or other manually produced image (although notably, it does not address the use of images of lookalikes, such as the example of a photo of the actor Woody Harrelson being used by police in New York to search for a suspect that they thought resembled him); (iii) to create a record that describes an individual's exercise of their First Amendment rights; or (iv) as the sole basis to establish probable cause in a criminal investigation. (However, results of a facial recognition search may be used in conjunction with other information and evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation.)

- **Exemptions from the law —** The bill does not apply to the use of a facial recognition matching system by the department in charge of issuing driving licences, nor to situations where a federal agency is involved.

- **No task force —** The proposed text of the bill aimed to establish a task force to study and provide recommendations on several issues arising from the use of FRT, but this section of the bill was vetoed by the Governor as it did not have an allocation in the budget.

State of Colorado

Colorado has enacted a very detailed facial recognition law which regulates its use by law enforcement agencies, and also other local government agencies. The Senate Bill 22-113 was adopted in May 2022 and it came into force in August of the same year.[583]

The structure of the law is very similar to the law enacted in Washington. While the rules are almost the same, there are differences in certain rules and in the wording of the legal provisions. The similarities are as follows:[584]

- there is an obligation to prepare and file a **notice of intent and accountability reports**;
- **meaningful human review** and testing must be in place in case of any decisions that can produce legal or similarly significant effects concerning individuals;
- in order to **mitigate performance discrepancies**, service providers must make the technical capability available to enable accuracy tests;
- **training** of individuals who operate the FRT must be organised;
- the deploying agency must maintain **records** sufficient to facilitate public auditing;
- the deploying agency must disclose its use of a facial recognition search on a **criminal defendant** prior to trial; and
- deploying agencies and judges must **report** the required information on their involvement in FRT use.

There are, however, some points in which the Colorado bill departs from the Washington bill:

- The content of the **accountability report** is slightly different, as the Colorado bill does not require the report to contain information on how the service provider and the agency intend to fulfil security breach notification obligations. The Colorado bill also regulates for limited situations when the agency does not have to prepare a report (largely when the use of facial recognition will be for commercial and not governmental purposes).
- Ongoing **surveillance**, including real-time or near real-time identification and persistent tracking, is allowed under somewhat different conditions than in Washington State, i.e. only if (i) there is a warrant; (ii) there is necessity to develop leads in an investigation; (iii) the agency has established probable cause for such use; or (iv) the agency obtained a court order authorising the use for the sole purpose of locating or identifying a missing person or identifying a deceased person.

» The bill does **not** expressly regulate or mention **predictive law enforcement tools** (although prohibition of predictive policing could be implied by interpretation of the law), nor does it regulate that facial recognition cannot be used to identify an individual based on a sketch or other manually-produced image.

» **Exemptions from the law** are somewhat different. The Colorado bill does not mention the exception of authorities in charge of managing driving licences. It does, however, regulate several situations in which the bill does not apply: (i) when the agency uses the facial recognition system in connection with a physical access control system in order to grant or deny access to a secure area (usually meaning biometric verification); or (ii) when the facial recognition system is used solely for research purposes by a state agency, so long as the use does not result in or affect any decisions that produce legal effects or similarly significant effects concerning individuals; or (iii) to a public utility company.

» The Colorado bill has a whole section about the use of **facial recognition in schools**. The general rule is that schools are not allowed to execute a contract with any vendor for the purchase of, or for services related to, any facial recognition service. There are two exceptions: (i) if the contract with the vendor was executed before the effective date of the bill, the exception is applicable only during contract validity; (ii) if the contract regulates a generally-available consumer product, including a tablet or smartphone, that allows for the analysis of facial features in order to facilitate the user's ability to manage an address book or still or video images for personal or household use.

» The Colorado bill establishes and regulates the membership, duties and obligations of a **task force** in charge of evaluating the use of FRT by Colorado agencies, with a mandate to examine and report the extent to which agencies are currently using FRT, and to provide recommendations for future uses, in a manner regulated in the law.

Commonwealth of Virginia

In a two-phased legislative process, the Commonwealth of Virginia has enacted an elaborate legislation that regulates the use of facial recognition

by all law enforcement agencies, including university campus police departments and the Department of State Police. First, in April 2021, a law was passed to put what at that point amounted to a *de facto* ban on the use of FRT by law enforcement agencies.[585] The ban primarily consisted of a prohibition to use or to buy this technology without legislative approval first — and at that stage, the state lacked any authorising legislation.[586] However, after further debate, this law was soon replaced by a new set of rules in April 2022,[587] regulating the conditions under which FTR use would be permitted.[588] It has been argued by the ACLU and in the press that the new rules are too broad and leave many issues unregulated.[589]

These new rules, enacted via Senate Bill 741, define at the outset the fourteen "authorised uses" of FRT.[590] Several of the uses include situations when the technology would "help identify a person", including suspected criminals, victims of certain crimes, witnesses to a crime, missing or deceased persons, persons unable to identify themselves due to incapacitation, or persons reasonably believed to be a danger to themselves or others. Other cases include scenarios where help is needed to mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism, or to determine whether an individual may have unlawfully obtained a driving licence, financial instrument, or other official form of identification. This list of use cases is far broader than the exceptions listed in the EU's AI Act, criticised by the EU's data protection supervisory authorities for being broad enough to allow general use.

Furthermore, the Virginia bill requires an evaluation of the technology before it is used, which must have an accuracy score of at least 98% true positives (genuine matches) across all demographic groups. This score is provided by the National Institute of Standards and Technology as part of the Face Recognition Vendor Test.

This statistic may sound high, however in reality any surveillance system used on a mass scale — whether testing for COVID-19, profiling airline passengers, or identifying people by means of biometrics — can still have a very high number of errors even at 98% true positives. In fact, a statistical phenomenon called the "base rate fallacy" makes a certain number of errors inevitable. Moreover, without the accompanying rates of false positives (people who were flagged but shouldn't have been) and false negatives (people who weren't flagged but should have been), the true positive rate provides only one piece of the puzzle. The complex mathematics of

biometric matches are examined further in the Practice section of this book in relation to the use of FRT by the London Metropolitan Police.

There are also transparency requirements in the Virginia law, for example that law enforcement agencies must collect and maintain certain data related to the use of FRT and must also publish an annual report. According to the bill, any match made through FRT shall not be used in an affidavit to establish probable cause for the purposes of a search or arrest warrant. Penalty rules are also regulated: any FRT operator who violates the agency's or department's policy for the use of facial recognition technology, or conducts a search for any reason other than those authorised by the bill, is guilty of an appropriate misdemeanour.

The bill also regulates several cases where the use of such technology is prohibited. These include: (i) the use of FRT for tracking the movements of an identified individual in a public space in real time; (ii) creating a database of images using a live video feed for the purpose of using FRT; or (iii) enrolling a comparison image in a commercial image repository of a FRT service provider except pursuant to an authorised use.

Finally, according to the bill, before a facial recognition system is put in use, a policy must be developed to regulate investigative uses, training requirements and certain usage protocols. The State Police released a model policy to guide law enforcement agencies in the further use of FRT. Police departments can either choose to adopt this policy or develop their own with stricter guidelines.[591]

State of Maine

The law that regulates facial surveillance, including technologies for analysing facial characteristics such as the iris of the eye, was enacted in July 2021.[592] At the time it was described as the "strongest statewide facial recognition law in the country", especially in contrast with its predecessors, which at the time mostly referred to Washington State.[593] According to the definition from the law, facial surveillance means "an automated or semi-automated process that assists in identifying or verifying an individual, or in capturing information about an individual, based on the physical characteristics of an individual's face".

This definition would cover a wide range of use cases including identification (i.e. of a natural person) and any form of categorisation or profiling on the

basis of physical characteristics. It is arguably broader, therefore, than the EU definition in the GDPR, which covers only data that have undergone specific technical processing and can allow or confirm the identification of a person. However, while it suggests that other facial features like irises, or the prediction of emotions based on facial expressions, could be included in the definition of "physical characteristics of an individual's face", other bodily or behavioural biometrics seem not to be covered.

The law, enacted via Maine Revised Statutes, Title 25, Chapter 701, regulates the use of facial recognition not only by law enforcement agencies, but by any state or local government. The basic rule and starting provision of the law is that no public official or body may obtain, retain, possess, access, request or use a facial surveillance system or information derived from it, or enter into a contract to that effect, or issue any permits that allow any of the stated actions to any third party — subject to a few expressly-regulated exceptions.

One group of exceptions to this basic prohibition are in place for the purposes of (i) investigating a serious crime (as defined in the law itself), when there is probable cause to believe that an unidentified individual in an image has committed the serious crime; (ii) assisting in the identification of a deceased person; or (iii) assisting in the identification of a missing or endangered person. Therefore, in these cases public authorities may use FRT without a court order. These exceptions are somewhat similar to the exceptions in the EU's AI Act and the withdrawn Serbian internal affairs law, which models its uses on the AI Act, both of which are discussed elsewhere in this book, although the proposed EU Act still requires judicial authorisation.

Furthermore, if FRT is used for these purposes, public agencies cannot perform facial recognition searches themselves, but must request a search by a competent institution, such as the Bureau of Motor Vehicles, FBI, or a state agency that issues government credentials. This is subject to further rules on how and under which conditions such searches can be made and recorded. The law also regulates that the State Police and the Bureau of Motor Vehicles shall maintain logs (with elements regulated in the law) that track all requests for searches of facial surveillance systems received and performed. Whilst searches by a state or federal agency at least imply that the underlying databases have been compiled on the basis of reasonable suspicion or criminal activity (although this may not be the case in practice), the fact that the Bureau of Motor Vehicles can undertake a search means

that every driving licence holder is put in the virtual line-up. Searches made on such basis have been criticised elsewhere, for example by the civil society organisation Statewatch concerning a proposed EU cross-border data sharing regime, the Prüm II Regulation.[594]

The law provides another group of exceptions from the general facial surveillance prohibition. This includes various specific situations, such as obtaining, maintaining, or using a facial surveillance system within the Bureau of Motor Vehicles in accordance with rules that regulate driving licences, or for the purposes of fraud prevention or investigation; using facial surveillance technology that analyses a person's iris in a regional jail or county jail; and for user authentication (such as unlocking a personal device). The law also confirms that the following use cases would not be considered banned uses: using social media or communications software or applications for communicating with the public, as long as such use does not include the affirmative use of facial surveillance; and using automated redaction software, as long as such software is not capable of performing facial surveillance.

One provision of the law that regulates allowed uses is permission for government entities to use evidence that has been generated from a FRT search and is related to the investigation of a specific crime. The wording of this provision is so broad that it begs the question: what are its limits in practice? Indeed, it seems that it can be interpreted to include different scenarios which would effectively circumvent the principle ban on which the whole law is based.

According to the law, facial surveillance data does not, without other evidence, establish probable cause justifying arrest, search or seizure.

Finally, the law regulates several enforcement rules if a violation has happened. Pursuant to these, facial surveillance data collected or derived in violation of the law must be considered unlawfully obtained and, except as otherwise provided by law, must be deleted upon discovery; and will constitute inadmissible evidence in any proceeding before public authorities. A person injured or aggrieved by a violation may bring an action in a court against the violating public authority. A public employee or official who, in the performance of their official duties, violates the law, may be subject to disciplinary action.

State of Utah

Utah enacted its FRT bill in March 2021 regulating the use of facial recognition by any state government body.[595] The law aims to regulate — instead of ban — FRT, which has already been in use in Utah and was met with some citizen support.[596]

Similar to the rules in Maine, a law enforcement agency cannot perform the search itself, but must submit a request to the competent state authority (here, the government entity that manages the image database, or the Department for Public Safety, if the image database is maintained by or shared with this department). The law regulates that trained and authorised employees can complete search requests only if the request is for a purpose allowed for in the bill; if the request includes a case identification number; and when it is a request made for the purpose of investigating a crime, that it specifies the crime and factual narrative to support that there is a fair probability that the individual who is the subject of the request is connected to the crime.

According to the bill, the agency can file a request for a facial recognition comparison for the following purposes only: (i) investigating a felony, a violent crime or a threat to human life; or (ii) identifying an individual who is deceased, incapacitated, or at risk and otherwise unable to provide the law enforcement agency with his or her identity.

Once a trained employee receives a request from a competent department, the search must be done in accordance with procedure that is regulated in detail in the bill. Pursuant to the provisions, if the facial recognition system indicates a possible match, the employee must make an independent visual comparison to determine whether the facial recognition system's possible match is a probable match. If the employee determines that there is a probable match, he or she must seek a second opinion from another trained employee or their supervisor. If they agree that the match is a probable match, they will report the result to the requesting law enforcement agency through an encrypted method. They must only return to the requesting law enforcement agency a result that all employees agree is a probable match. If, however, the second trained employee or supervisor disagrees that there is a probable match, they shall report to the agency the fact that the search returned no results.

When submitting a case to a prosecutor, a law enforcement agency must disclose to the prosecutor whether a facial recognition system was used in investigating the case, and if so, a description of how it was used in the investigation.

Any government entity, including law enforcement agencies, must notify the public in advance about their FRT use practices, in accordance with the rules set out in the bill. In addition, upon request, a government entity must release statistical information regarding facial recognition comparisons. They must also prepare annual interim reports to the competent government committee (excluding details regarding a pending investigation).

The bill explicitly regulates that a government entity may not use a facial recognition system for a civil immigration violation, and as such is the only US state whose FRT laws explicitly acknowledge the particular harms for minority communities.

Commonwealth of Massachusetts

The state of Massachusetts has enacted legislation that regulates some matters related to the use of facial recognition by law enforcement agencies, but with limited scope. The rules were made in the course of the police reform in 2020 and became legally effective in July 2021.[597] Although the state initially intended to pass broad rules on the matter, due to political backlash,[598] the provisions enacted only address the use of face recognition to search images and identify a person in a database.[599]

Namely, according to Section 220 of Chapter 6 of the General Laws, law enforcement agencies must get a court order before running a face recognition search, except in two situations: when they search for a deceased person, or when the agency reasonably believes that an emergency involves substantial risk of harm to an individual or group of people. With respect to the latter situation, the law regulates in detail that the order must be issued by a court or justice authorised to issue warrants in criminal cases, based upon specific and articulable facts and reasonable inferences therefrom that provide reasonable grounds to believe that the information sought would be relevant and material to an ongoing criminal investigation or to mitigate a substantial risk of harm to any individual or group of people.

Once these conditions are met, the agency cannot perform the search themselves, but must have someone from the state police, the FBI or the Registry of Motor Vehicles perform the search.

Transparency is required under the law. The agency must document each facial recognition search performed and provide documentation quarterly to the executive office of public safety and security. The minimum reporting elements are also regulated. The executive office must publish annually on its website documentation received from law enforcement agencies with a regulated list of minimum information.

Finally, the law has a couple of provisions that clarify under which circumstances the use of facial recognition tools would be allowed. Pursuant to the law, a law enforcement agency may use FRT for the sole purpose of user authentication on their devices. Furthermore, an agency can use automated video or image redaction software if such software does not have the capability of performing facial recognition, and it can receive evidence related to the investigation of a crime derived from a facial recognition system if such a system was not knowingly obtained in violation of the law by public agent or public official.

This legal framework was met with criticism. The American Civil Liberties Union (ACLU),[600] which sought to ensure the protection of rights in the legislation, argues that the current law does not sufficiently protect people and their rights, especially from the perspectives of racial justice, privacy, due process and civil liberties.[601] In 2021, the ACLU initiated a campaign for legal changes that would use the initial rules as a starting point and make a more comprehensive "Act to Regulate Face Surveillance".[602]

Finally, in the course of this police reform, a "Special Commission"[603] was created with the task to study facial recognition technology and make recommendations for future rules regarding its use.[604] The Commission issued a report in March 2022, which lists 13 recommendations. Out of these, the recommendation that facial recognition software should be used only with a court warrant based on probable cause that a person has committed a felony seems to be the biggest departure from current law (while some limited exceptions would be acceptable and strictly regulated). Recommendations also include banning the use of facial recognition for live surveillance or tracking, as well as for "emotion recognition". These recommendations sparked further debate, as it has been suggested that

proposed rules would prevent the police from using the technology in a meaningful and useful manner, while the privacy concerns remain.[605]

State of Alabama

Senate Bill 56, Alabama's law to regulate facial recognition, was passed in April 2022 and came into effect in July of the same year.[606]

Initially, the proposed text of the bill had three components:[607] (i) to prohibit law enforcement agencies from using a facial recognition match as the sole basis of probable cause or arrest; (ii) to prohibit them from using artificial intelligence, or a facial recognition service,[608] to engage in ongoing surveillance except for in certain circumstances; and (iii) to prohibit artificial intelligence or a facial recognition service from being used as a way to identify an individual based on other images (if this text had been adopted, it seems it would have been challenging to interpret the exact meaning of this prohibition).[609]

However, following amendments, the final text regulates only the first component. According to the bill, a state or local law enforcement agency may not use FRT match results as the sole basis to establish probable cause in a criminal investigation or to make an arrest, and that for the said purposes, match results can be used only in conjunction with other lawfully-obtained information and evidence.

There is no available information about the reasoning for the amendments to the initial proposal, nor why the adopted text has such limited scope. One speculation is that the main issue that urged regulation was the need to address the key public concern about the possibility of misidentification.[610] This might be correlated with the news that, before the law was proposed, there were reports of Alabama police using facial recognition to identify Capitol riot suspects, with Clearview AI involvement.[611]

State of Vermont

In October 2020, Vermont passed a law that outright bans the use of facial recognition technologies by law enforcement at the moment, i.e. establishes a moratorium on its use until further legal action.[612] According to bill S.124, Sec 14, a law enforcement officer shall not use facial recognition technology or information acquired through the use of facial recognition technology — until the use of facial recognition technology by law enforcement officers is authorised by an enactment of the General Assembly of Vermont.[613]

However, the strict ban was revisited in 2021 upon the initiative of the Attorney General, who called for an exception for the use of facial recognition by police in investigations of child sexual abuse.[614] The exception came in the form of bill H.195, according to which the General Assembly authorised the use of FRT by law enforcement during a criminal investigation into the sexual exploitation of children. This technology can be utilised only where law enforcement is in possession of an image of an individual they believe to be a victim, potential victim, or identified suspect in the investigation, and the search is solely confined to locating images, including videos, of that individual within electronic media legally seized by law enforcement in relation to the specific investigation.[615] Despite this, the Vermont ban is nevertheless far more restrictive when it comes to the use of facial recognition technologies by police, particularly for mass surveillance purposes, compared to other US states.

According to the information available on the Vermont Government website, a Facial Recognition Technology Working Group is to be established,[616] as mandated under bill S.124, with the mandate to analyse the risks and opportunities with respect to FRT use by law enforcement agencies, and to make recommendations about potential future authorising enactments — presumably in the same vein as bill H.195.

Commonwealth of Kentucky

The facial recognition law was signed in April 2022 in the form of Senate Bill 176.[617] This bill does not set directly applicable rules on the use of facial recognition technologies, but rather establishes a process to create statewide standards and requirements for law enforcement. [618]

According to the bill, a working group on facial recognition technology is to be created. Membership of the working group is regulated in the bill, as well as its duties and competence. The primary duty of the group is to create and make publicly available a model policy for use by law enforcement agencies, on or before 1 January 2024.

The content of the model policy is regulated in detail, and includes inter alia: (i) a specification of the authorised uses of FRT consistent with the law (including how search results relate to establishing probable cause for arrests, as well as the prohibition of using the technology to identify a person participating in constitutionally protected activities in public spaces), as well as requirements for law enforcement agency employees that

are authorised to use FRT; (ii) a requirement for a law enforcement agency to specify a process for the agency to document instances in which FRT is used; (iii) procedures for the confirmation of any initial findings generated by FRT by a secondary examiner; (iv) data integrity and retention policies, as well as data security measures, training procedures and processes; (v) a minimum accuracy standard for face matches in all demographic groups to ensure non-discrimination; and (vi) a mechanism to produce a record of prior uses of FRT that can be used for audit and verification.

The policy must also establish a process that requires an agency to compare a publicly available or lawfully acquired image against a database of publicly available or lawfully acquired images. One unusual requirement in the law is that the policy must specify a process that addresses the privacy of persons by excluding, redacting, blurring or otherwise obscuring nudity or sexual conduct involving any identifiable person.

A law enforcement agency that uses FRT must have a use policy in place prior to using the technology and must file a full copy of its policy or any revision of its policy with the Justice and Public Safety Cabinet within thirty days of the adoption or revision.

The bill did not give rise to much public debate, based on available information, perhaps because the rules are yet to be defined when the model policy becomes available. At the time of writing, that was still not the case.

CASE LAW

Since laws regulating the development, deployment or use of facial recognition by law enforcement agencies in the US emerged only recently, there are still no court decisions regarding their application that would help with interpreting the legal requirements, or even the constitutionality of those laws.

However, there have been several cases of FRT misidentification that ended up in court. In 2021, a man named Robert Williams sued the Detroit Police Department for wrongfully arresting and jailing him based on an incorrect match from their facial recognition system. The court judgement on this case is still pending.[619] This is not the only time an arrest has been made in such circumstances,[620] but we still have to wait and see what case law practice will emerge from these types of situations, at a state and federal level.[621]

When it comes to the use of facial recognition by federal agencies, there is a significant pending case initiated by the ACLU in 2019. The organisation sued the federal government in order to get details on its face surveillance practices, including the use of facial recognition technology by the FBI and the Drug Enforcement Administration (DEA). In January 2019, the ACLU first submitted a request for public records, and while the FBI and DEA each confirmed receiving the request, neither agency provided any information in response. The lawsuit claims that "responsive documents would inform the public about how face surveillance technology is currently used by the government, and what, if any, safeguards are in place to protect core constitutional rights".[622]

The case law on commercial uses is much more developed since laws that regulate such uses (like Illinois' BIPA and Texan CUBI) first appeared more than a decade ago.

Under BIPA rules, Clearview AI has agreed to a new set of restrictions under a legal settlement made before the Illinois state court in March 2022. According to the settlement, Clearview AI is prohibited from providing access to its face recognition database to any state or local government entity in Illinois, including law enforcement, for a period of five years (which means they cannot take advantage of BIPA's exception for government contractors during that time). Restrictions are even stricter when it comes to private entities, and include a ban on Clearview AI granting paid or free access to its database to any private entities nationwide (not only in Illinois), subject to narrow exceptions contained in BIPA.[623]

Commercial cases for various violations of privacy via FRT use have mostly end up being settled.[624] Most notably, there was a $650 million settlement with Meta in 2021, again under BIPA rules.[625] A similar case in Texas under CUBI rules was initiated by the Texan government against Meta in early 2022, and is still ongoing.[626]

In 2021, TikTok was a party to a BIPA settlement for $92 million regarding their facial recognition practices.[627] Snap, the parent company of Snapchat, agreed to a $35 million settlement in 2022 (for the use of facial recognition within "Lenses" and "Filters" Snapchat features),[628] while at around the same time, Google settled for a round figure of $100 million (based on allegations that Google Photos gathers data on facial geometry to identify similarities and variances between people and offers a function to group images of similar faces together in violation of the BIPA).[629]

ZIMBABWE

What type of act regulates processing of biometric data

National constitution
Yes, the right to privacy (home, possessions, and communication).

Data protection law
Yes, the Data Protection Act, 2021.

Defining and regulating facial recognition

Data obtained through Facial recognition is regulated as personal data.

Details

Specific use cases defined

- The use of biometric data is regulated under specific article of the Data Protection Act; the processing is allowed only if there is an appropriate legal basis.

Specific authorities defined

- The Postal and Telecommunications Regulatory Authority serves as a supervisory authority; it can issue opinions and guidance and is in charge of handling complaints and investigations, but cannot issue penalties.

ZIMBABWE

CONTEXT

The political climate in Zimbabwe during the rule of Robert Mugabe, which lasted over 30 years, turned the country away from the West and towards Chinese influence.[630] The Mugabe regime led the country to economic and democratic demise over the years. A change of power occurred in 2017 after the coup d'état, and Emmerson Mnangagwa was elected president the following year. However, under the rule of the new president, Zimbabwe continues to be on a path of "democratic regression" and "the country's civic space is shrinking both online and offline as the regime employs a raft of legal and extra-legal measures to thwart dissent".[631]

The Chinese influence came in the form of financial aid, but also with the heavy participation of Chinese companies (most notably Huawei) in the construction of internet and telecom infrastructure in Zimbabwe.[632] The new parliament building, opened in 2023, was fully funded by China as a "gift" to Zimbabwe.[633] The Chinese involvement in various procurement contracts is significant, in particular when it comes to modern surveillance technology, which reportedly also includes facial recognition technology for the purpose of law enforcement.[634]

In 2018, when president Mnangagwa visited China, there were speculations that FRT would be purchased from a Chinese company, *Cloudwalk Technology Co.*[635] That same year, the government initiated "The Zimbabwe Smart Sustainable Cities Initiative",[636] which was linked to plans to deploy facial recognition tools in major cities,[637] as well as Chinese plans to use cooperation with countries like Zimbabwe to train their technology with a "black population".[638] According to

some reports, the installation of FRT at the borders was already launched in 2018.[639] Other reports suggest that in 2020, cooperation began with Huawei, CloudWalk Technology and Hikvision for the procurement of FRT.[640] CloudWalk Technology is "already harvesting the data of millions of Zimbabweans under biometric voter registration for storage and processing in China".[641]

The most recent project linked to the use of facial recognition is called "Zim Cyber City", in the area of New Harare – planned as the new seat of government and built at the outskirts of the existing city of Harare.[642] The project was launched in 2022 and is still in very early stages of development. However, the main investor – Dubai-owned company Mulk International – already announced that one of many "smart" features of the project will be "surveillance technology that is directly connected to law enforcement authorities", with the aim of ensuring the "safety of people living and working there".[643] We shall have to wait to see how this project will unfold, as well as how the UAE's interest in the development of facial recognition-based technology will play out in a much poorer country such is Zimbabwe.

Even though there are many reports and indications that public bodies in Zimbabwe are already using FRT, or at least collecting their citizens' data to develop this technology, there are no clear proofs of such practice, its magnitude or scale, which might be a problem in itself.

LAW

The Constitution of Zimbabwe regulates the right to privacy in its Section 57, which includes protection over citizens' homes, possessions and communications, but does not mention protection of any personal data – with the exception of health data that are explicitly protected from disclosure.

The law that regulates personal data matters was enacted in December 2021, but did not regulate the date of its entry into force.[644] The law was finally titled "Data Protection Act" (ZDPA), while during the legislative procedure its working title was "Cybersecurity and Data Protection Bill".[645] This was because it regulates matters related to both cybersecurity and the protection of personal data, and its text also amends Criminal Law (Codification and Reform Act), the Criminal Procedure and Evidence Act, and the Interception of Communications Act.[646]

This approach and the wording of many ZDPA provisions received criticism, as the new rules have a great potential to be used for political oppression – especially the cybersecurity portion of the law, such as rules on spreading false information that "undermine the freedom of expression and freedom of the media".[647]

Personal data protection provisions, on their face, seem to follow modern, EU-led, legal logic. The ZDPA has provisions concerning the legal basis for data processing, and regulates data subjects rights and the duties of data controllers and processors. The ZDPA applies to any organisation, including government entities. The Postal and Telecommunications Regulatory Authority (POTRAZ) is appointed as data protection authority in charge of enforcing the ZDPA.

When it comes to regulating biometric data, and more specifically facial recognition, the ZDPA does not go into too much detail. Moreover, biometric data are not defined in the law, and we can only assume that they would include facial recognition data (as facial recognition is not expressly mentioned anywhere in the law). It is also worth noting that the ZDPA does recognise sensitive data, but biometrics are not contained in this definition, which includes: (i) information that may reveal the racial or ethnic origin of a person, their political, religious or philosophical beliefs, membership of a professional or trade association, sex life, criminal educational, financial or employment history, gender, age, marital status or family status; (b) health information; (c) genetic information; or (d) any information which may be considered as presenting a major risk to the rights of the data subject. In the absence of official guidance or court practice, we can only speculate whether biometrics would fall into the last category of sensitive data. But for legal interpretation it is indicative that genetic and health information are expressly listed as sensitive data, while biometric data are not.

KDPR rules that deal with biometric data directly are contained only in its Section 12, which is titled: "Genetic data, biometric sensitive data and health data". An important aspect for legal interpretation may be that this title refers to biometric "sensitive" data, while the legal provision in paragraph 1 of this Article reads: "The processing of genetic data, biometric data and health data [...]", thus omitting the word "sensitive" from the legal provision. Could this imply that there are some biometric data that are sensitive and others that are not? Again, it is difficult to reach any conclusion without some official guidance.

Section 12 continues to say that processing of genetic data, biometric data and health data is prohibited without consent, or if one of the exceptions to prohibition apply. These exceptions include, inter alia, situations when the processing is necessary/required (depending on the exception): (i) in the field of employment law; (ii) to comply with national security laws; (iii) for the promotion and protection of public health, including medical examination of the population; (iv) for substantial public interest; (v) to protect the vital interests of an individual; or (vi) for the prevention of imminent danger or the mitigation of a specific criminal offence. There are also a couple of GDPR-inspired exceptions, such as if data have apparently been made public by the data subject or the processing is necessary for the defence of legal rights.

This list raises concerns due to several vague and broad exceptions that government bodies could use in the context of various agendas. This risk has been recognised by human rights lawyer Kelvin Kabaya, who claimed that this article was not compliant with the Constitution. In his statement for Global Voices, he said that "the proviso to the section [12] is couched in a very wide manner and is capable of being abused. Phrases such as substantial interest, are incapable of a precise meaning. This proviso may fail the constitutional muster, in that it is vague and may violate the right to privacy."[648]

Finally, section 12 regulates in some further detail the processing of genetic and health data, but does not mention anything else regarding biometrics.

One provision of the ZDPA that can potentially serve as a safeguard to some uses of facial recognition and other biometric surveillance tools is the regulation of automated decision-making, which is, again, inspired by the GDPR. According to Section 25 of the KDPA, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the subject or similarly significantly affects them. There are two exceptions to this rule: if the data subject consented to such a decision, or if the decision is based on a provision established by law. Strict interpretation of the second exception should mean that there should be a special law which would regulate the particular automated decision-making process.

Overall, it seems that the KDPA does not regulate the processing of biometrics in a comprehensive and satisfying manner. The lack of legal definition, openness for different interpretation of the nature of biometric

data, wide ambiguous legal grounds for their collection, and lack of any meaningful safeguards with respect to their use by public authorities are all causes for concern once the government starts implementing any of the announced facial recognition projects.

According to the POTRAZ website, there are currently no bylaws or guidance that address any aspects of biometrics processing.

CASE LAW

Courts in Zimbabwe have still not ruled on any issues related to biometric mass surveillance, nor has POTRAZ made any individual decisions on such matters.

One case may, however, be relevant in terms of what can happen in Zimbabwe when the government uses interception laws for its purposes. Namely, in 2019 protests broke out after the announcement that fuel prices would be increased by 150%.[649] The government's reaction was to shut down all internet in the country, by ordering telcos to cease providing their internet services.[650] The urgent legal reaction came from the Media Institute for Southern Africa and the Zimbabwean Lawyers for Human Rights, who filed a complaint to challenge the use of the Interception of Communications Act by the Government to completely suspend internet communications.[651] The High Court ruled in favour of the applicants, declaring that the respective government order (issued by the competent minister) was illegal, as it was not issued in accordance with the Interception of Communications Act. This ruling was based on the fact that it is the president, not the minister, who has the power to issue any orders of such kind. As such, the court did not have to decide on the merits in terms of violation of constitutional rights by government actions, including of the freedom of speech, nor did it rule on whether the Interception of Communications Act allows for such indiscriminate measures.[652] The result of this ruling was also that the telcos were ordered by the High Court to unconditionally and promptly resume full internet service.[653]

PRACTICAL

INTRODUCTION

This final section, focused on a series of real examples, brings the politics of facial recognition to the fore. Whilst the term "biometric mass surveillance" clearly covers any generalised use of such systems, it is vital that arbitrary uses are also considered under this umbrella. So too are databases and other parts of the technical infrastructure intrinsic to the conception of biometric mass surveillance, bringing us to a wide and encompassing definition. This is critical, because governments frequently claim that deployments are "targeted" as a way to try to avoid scrutiny.

Through the lens of harms, drawing on the work of Natalie Smuha and of Harini Suresh and John Guttag, this section emphasises the importance of looking at the damage caused by biometric surveillance not only on an individual level, but also at the macro all-of-society level. By resisting a techno-centric approach, and instead privileging a sociological approach, we are more able to recognise that every part of these technological systems, including the data that feeds them, are products of power and history.

This is evident in several of the cases studied, where the use of facial recognition by the state has formed a part of an apparatus of violence, such as in Myanmar and New York. Following repression by the junta-run government in recent years, protesters and political opponents in Myanmar were imprisoned and killed with impunity, in a persecution that was facilitated — and even empowered — by the use of facial recognition to rapidly identify and detain dissidents.

In New York, the long-running over-policing of Black and other racialised communities has been both exacerbated and obfuscated by the growing use of facial recognition technology. This theme of simultaneous visibility and opacity — for example the tension between the superficial visibility of the NYPD's body-worn cameras compared to attempts to cover up the outcomes and harms of these practices, such as false and politically-motivated arrests — plays out throughout this book.

Yet despite this toxic meeting of digital and analogue racism, there are examples of resistance in New York. Communities and non-governmental organisations like Amnesty International and the American Civil Liberties Union (ACLU) have been revealing these practices and litigating for more

transparency. And the report of the NYPD Comptroller, an independent supervisory authority, is one of the few examples anywhere in the world where the public have been provided with accurate and relevant information on the use of artificial intelligence systems by police. The case of Serbia brings further hope, where attempts to legalise the deluge of Chinese surveillance cameras that were quietly installed in the capital were met with strong public resistance, leading to the laws being dropped, at least for now.

Yet these use cases, deployed with claims of "national security", show a systematic conflation of national security and public safety use cases. They also raise the question of who is really safer when our faces and bodies are placed under permanent surveillance.

This question is especially pertinent when it comes to the surveillance of populations on the move. In Greece, border surveillance tech, including biometrics, has been linked to pushbacks of people seeking asylum — with funds supposed to be for COVID-19 recovery being secretly diverted into investments in monitoring systems. An enormous border surveillance industrial complex has underpinned many of these developments. The same issues are seen in Central America, where biometrics have facilitated efforts to block people from seeking asylum (a clear violation of international law).

In Palestine, we see perhaps the clearest example of how devices, software and databases fit together into a system of biometric surveillance and oppression which far exceeds the sum of their parts. In particular, this case study shows the limitation of an approach that looks at the harms created at various points in the socio-technical system. This is because the extent to which Palestinians have been put under biometric and other surveillance by the Israeli military — which even boasts a so-called "Facebook for Palestinians" — cannot be mitigated. Even the most technically "perfect" system would do nothing to minimise the routine control and oppression that are facilitated by biometric tools.

In the context of retail and services — both public and private — uses have brought the pervasive tracking of social media into the physical world. Despite regulators pushing back on the lack of any sufficient justification for the use of these systems, shops, banks and other services in Australia, the US and the UK have been keen to use them. In one example, a teenager was wrongly accused of shoplifting thanks to profiling facilitated by these systems.

Finally, the cases of the French Olympics and Paralympics and the London coronation of King Charles show the growing use of biometric systems to police and control public spaces and events. Despite claims to have leading data protection frameworks, both of these countries are experimenting with systems that track people who are either trying to enjoy a sports event, or a public celebration (or its counter-protest). The question of protest is especially pertinent for the UK, as the many deployments of live facial recognition — without proper authorising frameworks and with serious risks of discrimination raised — are accompanied by new laws which restrict several forms of protest.

In sum, this section viscerally highlights that the laws interrogated in the previous section are failing to keep people safe from the harms of biometric surveillance. Despite a shocking lack of evidence of their effectiveness, and a lot of evidence of their harms, governments and companies are fervently deploying biometric surveillance systems with inadequate regard for their consequences. These actions only serve to entrench existing power structures.

After detailed analyses of the technical characteristics of biometric surveillance and the laws that regulate (or not) its use in previous sections of this book, we can now delve into how these technologies are put into practice around the world. The use cases are vast due to governments and companies willingly experimenting with ways in which to use them, often before assessing all of the potential risks. This is especially true of the use of biometric technologies for purposes that amount to mass surveillance of populations, often operationalised under the guise of public safety and national security. Peter Könings argues that the current set-up of large-scale government surveillance of citizens has made these practices seem *prima facie* a lot less intrusive through the use of automated systems and other emerging digital technologies, which can sometimes make it harder for societies to grasp the extent of potential abuses and obscure the harms.[654] The truth, however, is that while the means through which residents are surveilled might be more covert nowadays, the scale and depth of these systems have increased exponentially compared to the past. Therefore, it is important to discuss the (so-called) ethics of biometric surveillance, and to look at the ways in which it is being implemented around the world, in order to understand more thoroughly how it is being justified and misused.

WHAT IS BIOMETRIC MASS SURVEILLANCE?

According to the Council of Europe, strategic or mass surveillance is an arbitrary form of surveillance aimed at preventing rather than mitigating dangerous practices, and is by nature more unselective than "targeted" surveillance such as phone tapping, bugging, etc., which generally requires some form of authorisation like a warrant.[655] In practice, mass use would translate to the employment of surveillance technologies to actively monitor populations as a form of control, rather than identifying a specific individual of interest who presents a clear and immediate threat to property, life and public safety in general.

One of the main characteristics of mass surveillance is that it is considered to be untargeted, which means that it does not only concern specific individuals of interest. Rather, it is defined by a non-selective approach that can span to gather the data of whole communities and even societies. Another important aspect is the means of collecting this data, which in the case of mass surveillance does not require suspicion or reasonable doubt to be put into use. Therefore, as is the working definition underpinning this whole book, biometric mass surveillance refers to the untargeted collection, processing, or analysis of biometric data, usually in publicly-accessible spaces. This kind of widespread surveillance can easily create a chilling effect on people, deterring them from participating in public life or curbing their freedom of expression and other fundamental human rights.

As the Italian Data Protection authority, the Garante Privacy, has explained, even when authorities are searching for a specific suspect, the fact that every person's data must be processed in order to determine whether or not they are the person being sought, means that this practice would still constitute (biometric) "mass surveillance".[656] This interpretation is truly important because many state authorities have incorrectly argued that searching for persons on a watchlist is "targeted" to justify the use of biometric systems in ways that nevertheless amount to mass surveillance.

European Digital Rights (EDRi) explains that remote biometric identification (RBI), such as public facial recognition, is one of the main pillars of biometric mass surveillance practices. RBI implies the use of biometric systems in public spaces in an untargeted or arbitrarily-targeted manner, which is inherent to the design of these systems, as noted by the Garante Privacy.[657] However, even in the European Union, which has made significant moves to restrict and regulate biometrics, and where a

majority of members of the European Parliament committed in 2021 to banning biometric mass surveillance,[658] there are still points of contention. The official position of the Council of the EU, adopted in December 2022, would allow police to use RBI in public spaces for a wide variety of reasons, and would not ban the use of RBI by other actors.[659] The document also provides a revision of the definition of AI systems as systems that are developed through machine learning approaches as well as logic and knowledge-based approaches. The move caused dissatisfaction amongst digital and human rights organisations with claims that the changes would soften regulators' understanding and subsequent approaches to the issue by essentially dehumanising these systems.

It is also important to reiterate that biometric mass surveillance practices are usually underpinned by large-scale data collection activities and expansive technological infrastructures, both hidden and in plain sight. These biometric mass surveillance infrastructures include databases that contain data from ID cards, medical records or other personal information stored in bulk by governments or private entities (such as the notorious Clearview AI, which has been discussed at length in this book).

These collections can hold vast amounts of individuals' data, but can get overlooked in the discussion of BMS because of their perceived lack of technological innovativeness — although the first section of this book has emphasised that in fact the mass gathering of biometric data is often at the cutting edge of surveillance. Current actions for collecting and processing biometric information are not the only pipeline for harm: pre-existing databases, compiled over several years or even decades, can equally present a dangerous breeding ground for privacy violations.

When used under the guise of security or safety reasons, they can more often than not be used to target specific groups such as people on the move, racialised people and other disenfranchised groups. In this sense, these databases are capable of exacerbating very particular and harmful types of over-policing and discriminatory targeting of certain groups, which become entrenched in the data and mistakenly read as "neutral". That is why it is so important that we consider arbitrarily targeted uses to also amount to biometric mass surveillance, because they are "targeted" in a manner that actually persecutes entire communities.

THE RISE IN BIOMETRICS

Biometric systems are becoming an unavoidable part of everyday life, from small-scale personal use (like unlocking phones) to their larger employment by private corporations and states. Governments and proponents of these technologies are quick to point out their purported benefits, which are mostly found in the necessity to protect public safety. Supporters of such biometric surveillance systems, which we argue would amount to mass surveillance, claim that their use by police is a crucial tool in preventing and detecting criminal activity. The argument is that the use of this kind of technology allows the police to intervene before a crime occurs, or to respond very quickly after it occurs, potentially saving lives and preventing harm to individuals and society as a whole.

Additionally, supporters of this non-targeted surveillance argue that it is a necessary response to the evolving nature of crime, which increasingly takes place in online versions of public spaces and across borders. However, there is a lack of evidence that biometric mass surveillance actually contributes to safer societies or higher rates of solving crimes.[660] Experts have pointed out that claims regarding the legitimacy and necessity of biometric mass surveillance are undercut by actual use cases. The majority of statistics which support the use of these systems are generalised and only rely on a small amount of actual data and completely forgo the human factor in the evaluation process.[661] On the contrary, court cases in 2019 in France and the Netherlands have shown that the reliance on facial recognition matches in court cases is deeply problematic and can even lead to cases being dismissed.[662]

One of the reasons for the lack of data on the effectiveness of such systems is that they are deployed in an opaque manner with limited public or institutional oversight. Anecdotal reports suggest that pilots that have been ineffective — which we can presume are the vast majority, as successes would likely have been highly publicised — tend to be quietly withdrawn, thus further preventing scrutiny. As these technologies have taken centre stage for governments promising to be tough on crime in the previous couple of years, concerns have continued to grow around how these systems are being deployed, as well as who is in charge of their upkeep and responsible distribution. Various ethical and human rights concerns surround these systems and the overall field of biometrics and biometrics-based data, their collection and subsequent (re)purposing.

In her paper "Beyond the Individual: Governing AI's Societal Harm", Nathalie Smuha argues that there is a difference between individual, collective and societal harms that can arise from the improper use of artificial intelligence systems like facial recognition.[663] Each of the three types of harm are unique in the ways that each one influences individuals and communities that can find themselves under government surveillance. Smuha argues that societal harms are the most widespread and detrimental for both individuals and communities, precisely because of the far reach of their potential harm for society as a whole. Societal harm is the sum of individual harms, such as individual acts of racial discrimination that can occur as a result of biased facial recognition technology (or the disproportionate use of these tools against racialised and minoritised people). This harm can infringe upon the rights of both individuals and communities, but ultimately Smuha argues that it must also be seen as harmful to human rights. She describes it as "harm to an interest held by society at large, going over and above the sum of individual interests" because of the structural and systemic nature of these harms.[664]

There is already a myriad of research conducted on the detrimental effects of mass surveillance for the expression and enjoyment of fundamental rights and freedoms, as well as the risks posed by under-regulated and non-transparent use of biometric technology.[665] In contrast, this research has not been sufficiently countered with anywhere near enough credible evidence in favour of the use of these technologies that could justify its use. It is also important not to lose sight of the effect that these technologies can have on human behaviour, including many different ways that they can be used to suppress civil liberties, such as in cases of crackdowns on protesters or the instalment of a social credit system.[666]

THE HARMS OF BMS

The biases in the training data and the design decisions of facial recognition tools, as explored in the first chapter of this book, have been a major concern for many civil society organisations as well as the members of society which they directly impact. There have already been multiple studies showing that AI systems are repeatedly less accurate at identifying people of different ethnicities, demographics and genders compared to the main historical subject of the training data — white, able-bodied men.[667]

This in turn can lead to a higher rate of false positives for minoritised groups, also including people with facial differences, and can contribute to perpetuating and reinforcing existing biases in policing and public administration, leading to discriminatory practices and outcomes. Critics argue that the use of facial recognition and other biometric surveillance tools by the police can erode trust in law enforcement, particularly in racialised communities that have historically faced discrimination and mistreatment.[668] In order to address these concerns, some have called for greater regulation of facial recognition technology and for police departments to implement policies and procedures that minimise the potential for bias and discrimination. However, others have advocated for an abolitionist approach, calling for these technologies to be divested from police entirely.

In EDRi's "Beyond Debiasing" study, a strong emphasis is placed on the ways that regulators and technology companies that produce AI-based systems choose to approach bias from a purely technological standpoint.[669] The study argues that various prejudices and inequities that can be embedded in facial recognition and other AI-based systems are oftentimes overlooked by decision-makers. Instead, the focus is placed more on "bias" as a mathematical problem to solve, which can result in discrimination by these systems being regarded as nothing more than statistical errors and technical issues.

However, this techno-centric approach essentially nullifies the role of structural discrimination, which is ever-present in the societies in which these systems operate daily. Ultimately, this kind of approach "squeezes complex socio-technical problems into the domain of design and thus into the hands of technology companies".[670] Among the key issues is that civil society, privacy advocates and other human rights activists are often excluded from conversations about the safeguards surrounding facial recognition technology and AI-based systems — let alone about whether or not they should exist in the first place. This exclusion significantly hinders the official conversations around biometric technologies, because it lacks the critical perspectives of actors who are on the front lines of protecting civil liberties.

Suresh and Guttag discuss the "seven sources of harm in machine learning", which are the key points at which biases and other harms enter into the entire lifecycle of machine learning systems.[671] These sources of harm are crucial for understanding and expanding the conversation related to the

use of biometric mass surveillance by authorities. In many instances, bias is discussed at a very surface level, which allows the beneficiaries of such technologies to justify their implementation. By expanding on the nuances between the various types of harm that can exist within machine learning processes, and by politicising the very concept of "data bias" to show how data are in fact subjective artefacts embedded in the context in which they were created, Suresh and Guttag's work allows for a more thorough, socio-technical perspective on the ways that the misuses of such systems can be classified and potentially combated.

Historical bias, the first of Suresh and Guttag's sources of harm, is already one of the more recognisable categories in the discourse of bias, and refers to the ways in which previous knowledge is used to perpetuate what can be known as representational harm. This refers to enforcing stereotypes about certain groups of people in the population based on the incorrect assumption that historical data are neutral, and can have a significant negative impact on the ways in which these technologies later perform. Since the algorithms are being coded with these previous knowledge structures, historical inequalities and patterns of discrimination will therefore be encoded in the fabric of such technologies.[672] Because automated facial technologies are descendant from analogue photography, they are subject to the same biases that were present in the development processes of this technology. Research has shown that historical racial discrimination has been present from the very inception of photography, with camera settings and equipment being optimised to prioritise the accurate depiction of white skin.[673]

For instance, a 2016 study showed that word embeddings that have been trained on Google News articles were found to contain a number of gendered stereotypes.[674] Word embeddings are representations of text data that hold semantic meaning and are used as vectors for a number of machine learning and natural language processing (NLP) operations, and are therefore an integral part of the final product. In the analysed data, certain gender neutral words such as homemaker, receptionist, hairdresser and nurse were more likely to be associated with the word woman, while protege, skipper, philosopher and boss were associated with the word man. Automatically generated analogies that operate in a he/she dichotomy were also found to be highly biassed, with examples such as barber/hairdresser, pharmaceuticals/cosmetics and architect/interior designer. The corpus of texts analysed here feature more than three million words from news articles written by professional journalists. The results of the study concluded that

implicit and explicit gender bias was widespread in the selected data. The authors argued that future attempts to debias these systems may at least help in removing or lessening gender bias within society and help future research to become fairer.

The harm of representation bias, also known as sampling bias, deals with the under-representation of certain parts of the population in datasets on which these systems are later trained and ultimately enforced. The main areas of issue stem from the people for (or against) whom the systems are used not being sufficiently represented in the training dataset. For example, the dataset might fail to include racialised and minoritised people (even when the technologies are intended for use against them) and it might also overlook certain data. According to the National Institute for Standards and Technology (NIST) report, the algorithms that were analysed performed the best for male-labelled faces, while female-labelled faces, and especially racialised faces, were the least accurate.[675]

In their seminal work "Gender Shades", Joy Buolamwini and Timnit Gebru underline the ways in which automated facial analysis algorithms can perpetuate bias when determining peoples' gender and race.[676] By analysing these systems, the researchers found that the current facial recognition systems have higher error rates for darker-skinned individuals, especially women, as well as for women with certain hairstyles. The study revealed that artificial intelligence systems are not yet fully neutral and therefore are not equipped to address diversity within human populations, and require additional training and benchmarking for gender and skin tone. The research calls for greater accountability from commercial developers and governments in ensuring that facial recognition technology is not used to perpetuate bias or harm marginalised communities.[677]

Another harm is measurement bias, which refers to the definition of proxies used for the collection of data in a dataset. Proxies are features or measures that are used to represent certain concepts in a quantifiable manner, which in turn provide useful information for the dataset. This would mean that in the case of measuring a certain condition or phenomenon, a proxy would amount to reviewing and collecting already available information about that specific issue. This would then allow for the system to make a prediction on the given data and classify it within the dataset. For example, suppose a company uses a college degree as a proxy to evaluate a candidate's qualifications for a job. This proxy may not accurately reflect a candidate's actual skills or job-related experience. Candidates who did not attend

college but have relevant work experience may be unfairly excluded from consideration, while candidates who have a degree but lack practical skills may be overvalued. This can lead to measurement bias in the hiring process and result in a less diverse and less qualified workforce. This type of bias can raise issues when the proxies are too vague, or do not accurately represent the concept they are trying to define, when the accuracy of measurement is not being equally enforced across testing groups or when the methods of measurement differ from group to group. Critically, we note that these measurements are decided by humans — introducing yet another opportunity for harm based on the worldview, and therefore prejudices and assumptions, of these humans.

A 2016 ProPublica investigation analysed the Northpointe's Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool, which was used by the police and prosecutors offices in the US. They found that the algorithm that was used to evaluate defendants was more likely to predict higher recidivism rates for Black defendants, while white defendants were often mislabelled as less risk-prone than they actually were.[678] The risk assessments were made based on a score which was generated for each defendant by employing a questionnaire that would then make predictions based on the collected answers. This would plainly mean that the defendants' scorecards would contain information of prior offences that would put them in the risk-prone category. The questions asked can clearly be interpreted as racialised, given the vast disparity of arrests and incarceration rates in the US between non-white and white people.[679] It can therefore be concluded that the proxy was "differentially measured" for these communities since it involved a higher false positive rate due to the difference in policing practices in certain communities.[680] So for example, Black and Hispanic defendants were more likely to be labelled as risky since they were more likely to have a prior arrest or run-in with law enforcement. This type of "predictive bias" was also identified by developers and police officers that use such softwares.[681]

In the case of aggregation bias, the harm arises from one-size-fits-all models that can overlook certain specificities within the data. Underlying aggregation bias, as Suresh and Guttag explain, assumes that the input to label process is consistent across all of the data, and moreover that researchers might incorrectly assume that trends in aggregated data apply across individual data points.[682] This view might potentially overlook many hidden patterns or lack thereof and misclassify certain data in an effort to fit

into a universal and established system, which in turn can lead to inaccurate conclusions through trends and predictions. For example, when analysing social media posts via natural language processing tools, meaningful analysis can be skewed if cultural, social and other group-specific contexts are not taken into account. Instead, nuanced looks in the subsets of particular data can be mistakenly interpreted in an attempt to standardise the resulting datasets and thus generate potentially harmful results.

In a study analysing Tweets from Chicago youths involved in street gangs, researchers concluded that around 50% of the words used in the Tweets were incorrectly or not at all defined by online dictionaries and existing databases.[683] The research aimed to determine the differences between labelling speech as aggressive with direct threats, as insults, or as indicating grief or loss. The takeaway was that common NLP tools that are usually used for classifying online speech are not accurate or representative of particular subsets of the community, and would therefore be misinterpreted if they were to be analysed alongside dominant and standardised meanings and contexts. It was also determined that certain dialects were more likely to be overshadowed or simply not even labelled within existing datasets.

Learning bias, the fourth harm defined by Suresh and Guttag, can occur when a system starts favouring certain outcomes over others, which may lead to the exclusion of outliers or input information that may be viewed as an anomaly by the algorithms. Outlier data is less frequent by default, and as such may suffer inaccurate results when analysed by the system, which is based on statistics and probabilities. In machine learning, an algorithm is trained on a dataset to identify patterns and make predictions. As the algorithm makes predictions, its accuracy is evaluated, and any errors are used to update its parameters and improve its performance. However, this feedback loop can become self-reinforcing if the training data is biassed or the evaluation metrics are flawed. If the training data is biassed in favour of certain groups or outcomes, the algorithm will learn to make predictions that favour those groups or outcomes, even if they are not representative of the real world. This self-reinforcing loop can create a feedback loop that perpetuates and amplifies any biases present in the data, leading to a model that consistently produces ever more biassed predictions. If these biassed predictions are used to make decisions or inform policy, they can perpetuate and reinforce systemic biases and inequalities.

A Guardian investigation found that AI tools that are tasked with analysing and flagging inappropriate images posted on social media tend to suppress

images of female bodies.[684] These are not photos that are in any way sexually explicit or inappropriate, they just happen to feature parts of female anatomy. The tools would label images of female bodies such as women doing yoga as "racy", while images of men working out topless were not labelled the same way. When the algorithms, which were developed by Microsoft, Google and other major tech companies, were tested on patient images in medical databases, they would rate images that showed how to conduct a breast examination and images of pregnant women as "explicitly and sexually suggestive in nature".[685] These labels led to accounts being shadowbanned, i.e. the content was not removed from the platform but its reach was significantly limited due to the allegedly explicit content. Further investigation proved that depictions of bras were enough for the algorithms to produce an almost 100% accuracy score, which would lead to an image being labelled as "racy" or sexual. It is clear that through this decontextualisation of an article of clothing or a body part, based on preconceived gender biases, these AI systems have already learned to discriminate against and objectify certain parts of the population.

The fifth harm — evaluation bias in machine learning — refers to the presence of systematic errors or inaccuracies in the evaluation of a model's performance. It occurs when the evaluation metric or the test dataset, also known as benchmark data, used to measure the model's accuracy and effectiveness is not representative of the real-world scenarios where the model will be deployed. For example, benchmark data collected from commercial facial analysis tools can lead to biassed results and oversights for features such as gender and race, which can be the result of historical, representation or measurement bias. Additionally, the choice of benchmark data can also affect the model's performance, depending on the nature of the problem and the respective tradeoffs between different evaluation metrics. Misrepresentative benchmark datasets can lead to systems being unable to perform well when used on other subsets of data, thus further broadening the scope for potential harms in the process. To minimise the risk of evaluation bias, it is important to carefully select the test data and evaluation metrics, and also to consider the potential sources of bias that may be introduced due to the modelling process.

In their attempt to create an inclusive and intersectional training dataset that would aim to eliminate well known biases, Raji and others outlined some of the biggest current obstacles these systems face. While performing an audit of the benchmark data, a number of issues were identified, such

as the limitations of widely used markers, for instance referring to ethnic or racial categories or binary gender labels that would lead to the exclusion of certain parts of the population. The researchers also pointed out that benchmark datasets should clearly state the purposes of their use so as not to be misinterpreted and used in broader contexts, which could lead to overexposure of labelled data and overriding the limitations of the benchmark dataset's intended purpose.[686]

Deployment bias focuses on the human decision-making that can take part in the data interpretation process. Even though these systems are created and tested in a somewhat autonomous setting, once they are deployed, there are a number of factors that play into how they are put to use and who is responsible for evaluating and interpreting the collected data. This could be dependent on the governments, private entities and organisations that may be privy to the use of such systems. We would argue, therefore, that even facial recognition systems that are in theory flawless (whatever that may entail) would still suffer from the pitfalls of biases and harms, since previous experience has shown that police frequently deploy surveillance technologies disproportionately against racialised, migrant and poor communities.

Especially in cases of facial recognition technology employed in police use, there is not enough information on the human factor in the decision-making process. When analysing the Metropolitan Polices' rollout of live facial recognition cameras on the streets of London, Pete Fussey outlines that the statistics provided regarding the effectiveness of the system are strictly concerned with its technical characteristics. In other words, these evaluations do not take into account the false positives that arise as a result of incorrect identifications made by police officials when using these systems to investigate and solve cases of crime.[687]

It is important to note that it might not be possible to observe and confidently identify all of the biases that can show up in the cases discussed in this chapter, including due to the general issue of a lack of access to information by civil society. However, the intention is to try and demystify the various biases which might occur, and in some cases have already occurred, with the deployment of such technologies in the real world. The broader harms that can arise as a result of these biases will serve as a guide for the many problems that are still very present when we discuss the implications of the uses of these technologies, especially given the pervasive lack of proper oversight and regulatory red lines.

CASE STUDIES

In addition to discussing the technical characteristics and regulatory frameworks which develop in and around this technology, it is also important to analyse and contest their real-world applications. Since countries across the world are approaching the regulation of facial recognition, biometrics and personal data in a number of different ways, the following examples confirm that the deployment of such systems globally can be equally diverse.

The examples in this chapter do not represent an exhaustive account of what is happening in countries and regions worldwide, nor even in each of the areas of interest defined in the book. Rather, they serve as descriptors for developing a broader understanding of how these technologies are being deployed and the potential downsides, risks and harms. The aim was to find cases from different countries and regions, which include deployments that have affected different social, ethnic and religious communities, in order to observe these issues from as many perspectives as possible. Again, the claim is not that this is a representative sample, but rather a diverse sample which might help identify similar patterns, as well as differences.

The cases are divided into four overarching areas of interest which present the framework for analysis. Each of the categories will help provide a more comprehensive look into how these technologies are being deployed, as well as how they are being justified. Given that the main goal is to present as much available information on each case, it is important to note that some of the discussed cases have been investigated more in-depth than others and therefore have more particularities surrounding them. This does not mean that we believe that some of the cases are more important than others presented, and we have done our best to analyse each case as comprehensively as possible.

ORWELLIAN NATIONAL SECURITY

The protection of national security is among the most frequently invoked arguments for the development and implementation of facial recognition technology, and by extension, intrusive systems, the use of which amounts to biometric mass surveillance. The concept of national security is in most cases deliberately vague and is very adaptable depending on the issue at hand. As Lucia Zedner argues, the turn of the millennium, spearheaded by the 9/11 terror attacks, as well as subsequent attacks in London and Madrid, has contributed to the "normalisation of emergency powers" in the field of national security.[688] Security in this case becomes more of a practice rather than an end goal and can therefore be employed more laxly. Moreover, it has become impossible to imagine security measures as independent of some sort of surveillance. The interplay between security and surveillance overlaps in its similar usage tactics as well as purposes, such as the monitoring, influencing and control of movements.[689]

This framing of national security allows governments to justify their intended or ongoing use of surveillance technologies. Moreover, the argument for national security is often conflated with public safety — a goal which, while important, is not serious enough to permit the same exceptional measures as for genuine national security purposes. It is not difficult to understand why this tends to be the case, since this rationalisation allows for authority figures to expand their reach and justify infringements on privacy and personal freedoms. Therefore, mass surveillance is also touted as a surefire way to guarantee better safety in public spaces. To this day, there is still no substantial evidence of any correlation between dense surveillance of public spaces and a decrease in crime or improvement in public safety.

On the contrary, the results of various studies on the accuracy of these systems in use by authorities tend to show the opposite, with most people less safe under biometric mass surveillance.[690] The (lack of) accountability of tech companies should also be emphasised in these discussions, since they routinely utilise their for-profit orientations (for example, intellectual property protections, as discussed in the first chapter of this book) to evade responsibility. Access Now's report on the deployment of biometric surveillance technologies across Latin America notes that some of the companies behind these systems offer them to governments for free in order to test their capabilities without any regards to the human rights risks which they pose.[691]

THE CCTV COUP — CRACKING DOWN ON DEMOCRATIC PROTESTS IN MYANMAR

Facial recognition technology has played a significant role in the violent and deadly crackdowns on peaceful democratic protests in Myanmar following the military coup in February 2021. Peaceful democratic protests were triggered by the military's seizure of power and detention of elected officials, including Aung San Suu Kyi. It has been reported that the junta-run government uses facial recognition-capable CCTV systems to identify and track protesters both in real-time,[692] and in retrospect, leading to arrests, detention, imprisonment and executions.[693] These technologies are just one element in the junta's wider effort to establish the total digital surveillance of the population in Myanmar. This includes online censorship, internet shutdowns,[694] price hikes on data usage and phone calls, ordering communication operators to install surveillance technologies to intercept communications without sufficient cause, and significantly tightening requirements for SIM cards and IMEI registration.[695]

According to reports, three Chinese companies, namely Dahua, Huawei and Hikvision, supplied the authoritarian junta regime with CCTV cameras.[696] These companies have already been sanctioned by the United States for their role in enabling the Chinese government to carry out acts of genocide and oppression against Xinjiang minorities.[697] The implementation of the CCTV camera project was entrusted to two local companies, both of which

have close ties to the repressive apparatus of Myanmar. The Chairman of Fisca Security & Communication, one of the companies selected, is a retired Deputy Commissioner of the Myanmar Police Force. Naung Yoe Technologies, the other selected company, has a history of providing equipment to the military.[698]

The response of the military junta to the protests was stark and repressive. According to reports, more than 20,000 individuals were arrested, with over 17,000 still in detention.[699] Furthermore, it is estimated that several thousand protesters lost their lives at the hands of the oppressive junta regime.[700] To track down protesters, the junta matches biometric data from the input feed from CCTV cameras against the national ID database. CCTV cameras, which are capable of scanning faces and vehicle licence plates in public places, automatically alert authorities to those on a wanted list.[701] The military junta utilised this technology to identify and target individuals who participated in the protests, resulting in the detention and arrest of hundreds of citizens. Many of these individuals were subjected to torture and other forms of human rights abuses,[702] which in some cases is likely to have been facilitated by the use of biometric mass surveillance technologies.

The legal and regulatory framework governing the use of facial recognition technology in Myanmar is weak, with little to no oversight in place. The Electronic Transactions Law and the Computer Science Development Law were both amended in February 2021 in order to expand the mass surveillance of citizens. The former enables arrests of residents for undesirable online behaviour (primarily their activities on social networks), including but not limited to spreading false information or damaging foreign relations,[703] while the latter requires all internet users to register their real names and other personal information, making online anonymity virtually impossible.[704]

The international community has imposed sanctions on the military junta-run regime, military-owned companies, private companies, individual businesspersons, politicians and administrators. Although the impact of these sanctions is unclear, it is evident that they did not have a deterrent effect on the regime, which has only intensified its authoritarian crackdown against civil dissent.[705] The use of facial recognition technology and CCTV cameras by the junta-run government in Myanmar to target peaceful democratic protests constitutes a clear violation of privacy, civil liberties and

human rights. The weak legal and regulatory framework governing the use of this technology, coupled with the lack of oversight and accountability due to the authoritarian nature of the regime, has enabled the military junta to use this technology with impunity.

The case of Myanmar highlights a difficult truth — biometric surveillance technologies, which in embedded democracies are recognised as a potential threat to citizens' freedoms and rights, are often used by illiberal democratic and autocratic regimes around the world as a means of curtailing those very rights and freedoms.[706] The military junta in Myanmar used facial recognition technology for disproportionate surveillance purposes in order to identify and target peaceful protesters opposing the *coup d'état*. Surveillance technologies, deployed by political systems marked by deteriorating or non-existent rule of law, are often turned into tools for illegitimate crackdowns on basic civic and political rights, such as freedom of expression and assembly. The use of biometric mass surveillance technologies to persecute certain groups harks back to the very origins of these technologies, such as the first large-scale biometric identity programme being the use of fingerprinting for control by British colonists in India,[707] and early ideas of facial measurement being pushed by the Nazi regime.[708]

The global availability and wide acceptance of such technologies contributes directly to the global trend of deteriorating democratic values and practices,[709] as it further strengthens autocratic regimes. In certain parts of Myanmar, the situation on the ground can only be described as perpetual civil war, while in other areas it amounts to crimes against humanity.[710] As such, these facial recognition technologies are not only suited to consolidating the power of authoritarian states and strengthening their totalitarian grip on society, but also to streamlining war crimes and atrocities.

THOUSANDS OF CAMERAS IN BELGRADE

In Belgrade, Serbia, the fight to ban biometric surveillance technologies, particularly facial recognition, has been ongoing for four years. Civil society organisations and privacy advocates such as SHARE Foundation have strongly opposed the introduction of these systems, especially when taking into account the Data Protection Impact Assessment (DPIA), which was conducted by the Ministry of Interior in 2019.[711] After the DPIA was sent to the Commissioner for Personal Data Protection for review of plans to install facial recognition cameras across Belgrade, the verdict was that the assessment does not meet the formal and material conditions which are prescribed by the national Law on Personal Data Protection.

The Commissioner found the system to be insufficient on two counts and halted its implementation until an adequate DPIA was conducted.[712] According to the Commissioner's opinion, the unselective mass surveillance system being proposed by the Ministry of Interior could not be justified because it lacked a concrete purpose based on well-established facts. The biggest issue to date is that the government did not make a sufficient argument for the necessity for such a system, nor was it able to justify such an invasion of privacy.

The first publicly-noted case of the biometric-enabled cameras — similar to the models examined in the first chapter of this book — being deployed in the city was in June 2019.[713] But the biggest rollout of the cameras across Belgrade came in 2020 and coincided with the COVID-19 pandemic and the subsequent national lockdown that was put in place. Although this

made it easier for the police to install the cameras around the city, residents were diligently reporting the cameras and sending them to the Thousands of Cameras Twitter account, an initiative started by SHARE Foundation.[714] The aim of the initiative was to map out all of the surveillance cameras that were being put in place across the city and to raise awareness about the impending threat of living under constant surveillance.

The deployment of biometric-ready cameras embedded with facial recognition capabilities all across Belgrade has shed a light on the ways in which Chinese technology is showing up and getting put into use around the world; this is clearly seen in the case study on Myanmar. Chinese tech giant Huawei is the main supplier of surveillance for law enforcement in Serbia. This cooperation dates back to 2011, when the Serbian government and Huawei started talks on implementing a "Safe Society" project,[715] which would include a mass surveillance system deployment. In 2014, the two entities signed a joint Memorandum of Understanding.[716] The installation of 1000 surveillance cameras across 800 locations in Belgrade was announced in 2019 with a link to the "Safe City" project on Huawei's site. The page was quickly removed, but SHARE Foundation archived it in time.[717] This constituted a vital piece of the puzzle, which civil society otherwise would have had no access to, due to the systematically opaque practices of companies and governments regarding biometric surveillance.

Following the 2019 DPIA, the Ministry of Interior (MOI) submitted an improved version of their request to the Commissioner in March 2020.[718] The reworked version of the DPIA still did not meet the Commissioner's requirements for the justification of such a project, and was rife with arbitrary language. For instance, the DPIA showed plans for facial detection to be carried out on all persons walking through an area covered by the video-surveillance system, and for the police to use the system for profiling, even though it was unclear from the document what the profiling would specifically entail. Overall, the government once again was unable to provide a sufficient legal basis for processing biometric data collected through the surveillance cameras.

Necessity and proportionality are constantly absent in the Serbian government's rationalisation for putting into place such an invasive system. In September 2021, the MOI released a Draft Law on Internal Affairs which proposed provisions for the use of mass biometric surveillance technology in public spaces.[719] If passed, the law would make Serbia the first European

country to legalise and conduct indiscriminate surveillance of its residents in public spaces. SHARE Foundation submitted comments on the draft during the mandated public debate proceedings, pointing out that such a law would effectively legalise biometric mass surveillance.[720] The comments called for several articles of the draft law that deal with biometric surveillance to be immediately removed, as well as an introduction of a moratorium on the use of biometric mass surveillance technologies and systems. The draft law was rescinded only a couple of days later amidst wide public scrutiny.[721]

However, only a year later it was back to square one. In late 2022, the MOI again released a re-revised Draft Law on Internal Affairs,[722] along with a new Draft Law on Data Processing and Records in Internal Affairs,[723] and a revised draft DPIA.[724] Through the SHARE Foundation's analysis, it was determined that the risk of unselective and arbitrary surveillance and facial recognition practices were still not adequately addressed by the Serbian authorities. The new draft laws stipulated that biometric data of residents would be extracted and retained for a period of 72 hours, which implies that the process is unselective and indiscriminate, allowing for potential gross violations to residents' rights to privacy.[725]

Following public debates on the new draft laws, and thanks to a concerted effort from civil society organisations and help from the international community, including Members of the European Parliament, the draft laws were withdrawn from procedure by the end of 2022.[726] The government expressed a desire to further consult with experts in the field of data privacy and privacy issues in general before making any additional changes.[727] This signalled a positive step in the fight against biometric mass surveillance, not only in Serbia, but in Europe more broadly, as it showed clear dissatisfaction from the public and from democratic representatives, especially on the transparency and accountability that was lacking in such a high stakes endeavour.

SHARE Foundation, along with other civil society organisations and privacy advocates, is firm in its stance that the use of biometric mass surveillance technologies in the country should be prohibited. Since November 2020, civil society organisations across Europe, now numbering over eighty groups and including SHARE Foundation, have participated in creating a campaign that aims to ban biometric mass surveillance systems from public spaces.[728]

BIG APPLE BIOMETRICS: THE NYPD CASE

Some of the most compelling examples of the negative consequences of unchecked technology use are found in the United States, particularly with regard to the police force's implementation of facial recognition technology (FRT) in public spaces — one of the most prominent and potent forms of biometric mass surveillance. There are several accounts of innocent individuals from racialised groups, in particular Black men, being wrongfully identified and unjustly detained as a result.[729] Despite the swift adoption of FRT by many police departments, legislative bodies have been slow to establish a legal framework that would ensure accountability and transparency in the use of such technologies. As an illustrative example, this case study will examine the New York Police Department's (NYPD) use of FRT. The NYPD's procedures and policies have long been under public scrutiny and the subject of intense political debates due to their disproportionate targeting of minoritised groups.[730]

In analysing the NYPD's use of FRT, it is essential to consider the state's overarching legal framework and policies regarding the application of

machine learning programmes — or, more specifically, the lack thereof. As evidenced by the February 2023 report by the New York State Comptroller, New York City (NYC) public agencies including police lack ethical and legal guidelines for the use of machine learning programmes such as algorithmic modelling, facial recognition, and other software that monitors members of the public.[731] The report further clarifies that "[New York City] does not have an effective AI governance framework. While agencies are required to report certain types of AI use on an annual basis, there are no rules or guidance on the actual use of AI."[732] The lack of a shared framework has resulted in NYC agencies developing their own divergent approaches. The Comptroller's report highlights two main areas of concern: risk modelling in the child welfare system and facial recognition technology used by the NYPD.

The NYPD has been criticised for not maintaining a basic inventory of its AI tools and apparently not being fully aware of all the systems it employs.[733] While the NYPD asserts that it only uses AI systems approved by the National Institute of Standards and Technology (NIST), it did not review the results of the NIST evaluation of its facial recognition technology. The Comptroller's report also reveals that the NYPD did not establish a desired or acceptable level of accuracy for its facial recognition system.[734] Although the department purports to develop tailored policies and procedures for specific technologies, these are not specific to AI but are rather manuals for the use of any technological tools. This reflects poorly on the NYPD's ability and sincerity in putting effective safeguards in place and assessing the risks associated with the use of biometric surveillance technologies.

The Comptroller's report was one of rare instances where the public has been provided with accurate and relevant information on the use of AI systems by the police. Since the introduction of facial recognition technology (as early as 2011), the department has effectively shielded the public from any pertinent information on its use of FRT. While the NYPD's use of facial recognition may be opaque, numerous CCTV and body-worn cameras have become a visible and constant reminder of their system of mass surveillance of residents. Although "only" 6,000 CCTV cameras were reported in 2017,[735] current estimates put the figure at above 25,000 cameras[736] — an increase of more than 400% in just over five years. Moreover, the NYPD's body-worn camera programme is the largest of its kind in the US, with 24,000 uniformed police officers equipped with body-

worn cameras.[737] A hoard of video footage from around 50,000 cameras is therefore at the police's disposal, and can be used for biometric analysis.

The NYPD states that they use facial recognition technology to identify suspects whose images were captured while they were committing a crime.[738] However, they claim that a match does not serve as grounds for arrest, but is treated as a lead for additional investigative steps. The department also claims not to use facial recognition to monitor and identify people in crowds or at rallies. Furthermore, the video from body-worn cameras is not routinely submitted for biometric analysis, nor are images of unidentified suspects routinely compared to other government photo databases (reserved, purportedly, for cases related to terrorism).[739]

Nonetheless, the most cautious approach would be not to take this information at face value. It might even be more appropriate to consider information on facial recognition technology provided by the police as unreliable. For a start, the NYPD is actively fighting strategic litigation efforts aimed at shedding light on the actual practices and tools deployed by the police department.[740] Additionally, the NYPD has a poor track record of being open about its FRT operations and has even misled the public in certain instances, as we are about to explore. As a result, the public's trust and confidence in the department have been eroded, and its reputation has been tarnished.

Clearview AI, the company that scraped 30 billion images from Facebook and other social media sites and has provided NYPD with facial recognition technology, is extensively covered at multiple points in this book. However, it is worth additionally mentioning here because it is one of the worst examples of the NYPD purposefully misleading the public. The department downplayed its relationship with Clearview AI, even stating that it had no formal or informal relationship with the company. However, in 2021 it was exposed that the NYPD used this tool during an extensive trial period, and individual members of the police workforce continued using it even after the trial period ended.[741] Although the NYPD signed no contract with Clearview AI, the New York State Police did, and as reported, conducted more than 5,100 searches to generate potential leads.[742] Despite claiming that it does not use FRT on protesters, the NYPD is actively attempting to withhold information on biometric data gathered during Black Lives Matter protests.[743]

In 2021, privacy advocates uncovered a significant undisclosed fund for surveillance, revealing that the NYPD did not have to seek approval from the city council or any other municipal officials to use these funds. Since 2007, through its Special Expenses Fund, the NYPD has spent a staggering $159 million on various surveillance tools and services.[744] In 2014, the department spent $800,000 on a five-year contract with Israel's largest defence contractor, Elbit Systems, which provided mobile x-ray vans supposedly capable of scanning for weapons in vehicles from a distance of 1,500 feet. Despite warnings from health officials about potential cancer risks associated with this technology, the police managed to keep the public uninformed about its use.

The NYPD also obtained cell-site simulators from KeyW Corporation, also known as "stingrays", which mimic mobile phone towers and log the identifying information of any phone that connects to them, allowing police to easily track individuals without a court order.[745] Moreover, the department illegally maintained a database of minors' fingerprints despite this being in violation of state law, and continuously uploaded minors' mugshots to its facial recognition database.[746]

The public discourse surrounding the NYPD's use of FRT bears similarities to the NYC community's struggle to deal with the infamous stop-and-frisk policy — two practices which, in the hands of the NYPD, are ideologically intertwined. According to NYPD data, since 2002 there have been more than five million stop-and-frisk incidents. The large majority of searches were conducted on people of colour, and most people subject to these searches were innocent.[747] Mayor Bill de Blasio, who took office in 2014, vowed to get rid of this policy, and indeed, the number of stop-and-frisk incidents has decreased significantly.[748] However, a sharp drop in stop-and-frisk incidents was recorded prior to 2014, presumably because lawsuits were filed against the NYPD and also as a result of strong public criticism. Regardless of the drop in numbers, racial disparities remain high — young Black and Latino males account for only 5% of the population, compared to 38% of reported stops by the NYPD. It is not surprising that FRT, which has lower levels of accuracy for racialised people in general (and for women of colour in particular),[749] has been closely monitored by human rights and privacy activists. When thinking about this example through the frame of the seven harms defined by Suresh and Guttag, it is a powerful illustration of how every single one of the defined harms — and most pertinently the

historical and representation biases, evaluation bias and deployment bias — come together in a toxic cesspit of both digital and analogue racism.

In New York City, there is a discernible correlation between over-policing and over-surveillance, with body-worn camera surveillance being a prime example. A 2022 report by Amnesty International demonstrates that this also holds true for CCTV cameras, particularly in Black and Latinx neighbourhoods.[750] The report's analysis reveals that census tracts with higher concentrations of people of colour in the Bronx, Brooklyn and Queens are subjected to a greater number of publicly-owned cameras. Moreover, neighbourhoods with higher rates of stop-and-frisk incidents are associated with the deployment of higher numbers of CCTV cameras. The analysis has even identified routes that exhibit a markedly increased CCTV surveillance and a greater likelihood of stop-and-frisk searches. As Matt Mahmoudi of Amnesty International asserts: We have long known that stop-and-frisk in New York is a racist policing tactic. We now know that the communities most targeted with stop-and-frisk are also at greater risk of discriminatory policing through invasive surveillance."[751]

The public availability of data which confirms the disproportionate targeting of racialised groups has enabled activists to put NYPD's stop-and-frisk policy under public scrutiny. However, the relevant data on the use of FRT is now shielded from public access, leaving the public to rely on cherry-picked and potentially unreliable data "proactively" published by the police. For example, according to the NYPD, its facial recognition technology has only produced five instances of misidentification between 2011 and 2017. However, Supervising Attorney Jerome Greco of Legal Aid, an organisation that has represented clients in facial recognition cases and has been instrumental in forcing the NYPD to disclose 58 private contracts with surveillance companies, claims that the criteria for determining what constitutes a mismatch are unclear.[752] Another issue is the absence of any guidelines or standards regarding the images that police can submit for FRT analysis. In practice, a wide variety of "probe photos", including altered photos, artist sketches, and even photos of celebrity look-alikes are submitted for analysis. Due to the low quality of the suspect photos, the NYPD has even resorted to using photos of Woody Harrelson and a New York Knicks player in separate cases where officers believed the suspect resembled the celebrities.[753] The Surveillance Technology Oversight Project (STOP)[754] has obtained public records confirming that the NYPD used FRT on approximately 22,000 occasions from 2016 to 2019.[755] Despite the

NYPD's assertion that there have been no wrongful arrests, at least half a dozen lawsuits have been filed against the department for its use of FRT.

In 2020, Derrick Ingram, a prominent Black Lives Matter (BLM) activist, was accused of assaulting an officer by shouting into a bullhorn near the officer's ear. The police who arrived at Ingram's place of residence were reportedly holding a document called Facial Identification Section Informational Lead Report, thus inadvertently confirming that the NYPD used FRT on Black Lives Matter protesters.[756] The available evidence suggests that the NYPD, despite its official policies, used FRT to identify a BLM protester and seemingly fabricated a criminal charge to do so, while the warrantless military-style siege lasting four hours was seemingly used by the police force to send a political message to activists in the BLM movement.[757] Once the NYPD dropped the misdemeanour charge against Ingram, he filed a lawsuit claiming to be the victim of the NYPD's campaign of intimidation, harassment and manipulation, and that police relied on fabricated evidence as means of justifying the brutal crackdown.[758]

Whilst the state of New York does not currently have regulations in place that would have stopped this, as the legal section of this book notes, five US states (Washington, Colorado, Maine, Virginia and Alabama) prohibit law enforcement agencies from using a facial recognition match to establish probable cause in the way that seems to have been done by the NYPD in the case of Ingram. This example is further notable because, whilst many of Suresh and Guttag's harms were likely at play, it was an egregious deployment "bias" (although the word feels insufficient here to explain what occurred) that constituted the particular source of harm.

The confluence of several factors have contributed to the development of the NYPD's expansive surveillance system. The department utilised a covert funding stream to acquire advanced surveillance technologies and capabilities. Furthermore, the NYPD created its own procedures and guidelines for the use of such technologies, which has contributed to an opaque system, lacking in almost any transparency or accountability.[759] Many unknowns still persist regarding the efficacy of the NYPD's employment of facial recognition technology. Given the Department's history of impropriety, any data presented by the NYPD on this topic should be viewed as unreliable and selectively chosen until further proof is provided.

The New York case illustrates that the use of surveillance technology is likely to amplify existing racial disparities in the outcomes and effects of current policing practices and policies. Racialised communities are the target of over-policing and over-surveillance, which can create a chilling effect on the rights and freedoms of members from these communities — for example, how safe and free they feel to join a Black Lives Matter protest. This in turn increases the likelihood of misidentification for members of racialised communities (because they are statistically more exposed to inaccurate technologies), compounded by the fact that FRT is known to be prone to errors when identifying people of colour. The deepening of racial disparities seems to be an inevitable outcome of using technology to strengthen surveillance and intensify the policing of racialised and minoritised communities.

THE BANOPTICON: EQUAL DISCRIMINATION OF PEOPLE ON THE MOVE

In this chapter, we have already discussed how facial recognition technology and other forms of biometric (mass) surveillance particularly affect minoritised, racialised and disenfranchised groups. The situation is no different when it comes to surveilling national borders. Recurring refugee crises at EU and US borders have repeatedly demonstrated that those in the most vulnerable positions bear the biggest brunt of experimental technologies being rolled out under the guise of national security and so-called humanitarian protection.

While the implementation of the EU's biometric Entry Exit System (EES), which will facilitate easier border crossings for all Schengen Area residents, has already been postponed multiple times due to concerns about the risks of the system,[760] the same cannot be said for several active port and border surveillance systems that are being used to monitor people on the move, in particular refugee and migrant populations. Governments all over the world have been experimenting with the use of FRT and other biometric technologies at their borders, which often lead to populations on the move being unfairly profiled or having their personal data collected and stored without proper consent, and also risk leading to the criminalisation of even the intent to migrate (which amounts to a violation of international refugee law).[761] In many countries, the technology has also been linked to pushback practices, i.e. the collective expulsion of persons, usually before they reach a particular country or territory, often in very dangerous ways.[762] To compound this, studies have shown that across European countries, minoritised and non-Western immigrant populations were found to be at higher risk of discrimination and criminalisation by national policing structures.[763]

Scholar Didier Bigo (2005) problematises the concept of the "banopticon" to explain how particular social groups become subject to constant surveillance in relation to transnational security practices. As such, the banopticon posits the targeted group (minoritised people on the move)

as excluded from normalised societal structures because of their future potential for disruption (through profiling), which therefore leads to a valid exclusion and helps enforce their lack of free movement potential (a normative imperative of mobility).[764] This allows the structures of power to afford the majority a feeling of safety, despite the constant climate of fear and uncertainty that plague nation-states in their exaggerated thoughts of terrorist or other attacks on their sovereignty. The "othered" groups of populations on the move become over-policed in ways that the in-group will never be, putting the excluded groups at greater risk of dehumanisation practices, usually in the name of security.[765] Another key takeaway is that, contrary to the Panopticon, these structures are not centralised or homogenised, allowing them to cast a much wider net and use a variety of techniques to fulfil their intentions.

HYPERION AND CENTAUR: GREECE'S BORDER MIGRATION SURVEILLANCE POLICY

The border surveillance industrial complex has become an increasing reality for countries on the frontlines of mass migration.[766] In Europe, the primary point of entry for people on the move is most often Greece, and so the country has inadvertently been positioned as the testing ground for some of the EU's biggest government agencies to trial technologies and methods against people on the move. This includes the European Border and Coast Guard Agency Frontex, which deals with border and coastline security in EU-member and Schengen countries.[767] For years, more specifically since the 2015 migrant crisis, the country, as well as international policing agencies, have been scrutinised over their use of invasive surveillance technologies. The surveillance systems in use have also, as a rule, been deployed in non-transparent and harmful ways, often discriminating against asylum seekers and playing a part in massive pushbacks at sea, which amount to a violation of international refugee law. In 2022 alone, a study showed that there were over 200,000 illegal pushbacks from external EU borders, with Greece accounting for more than 26,000 cases.[768]

The ongoing harms that these systems pose for populations on the move are thoroughly documented and contribute to creating a hostile climate for people seeking to migrate to other countries for reasons such as war, famine, threat of persecution or economic issues. In a 2022 report, the Balkan Investigative Reporting Network (BIRN) concluded that Greece used pandemic-recovery funds supplied by the EU to implement two

new systems for monitoring people on the move and in makeshift refugee camps, which they have had in plan since 2020. The two systems, named Hyperion and Centaur, track the movement of people in and out of asylum camps in the country through use of behavioural analysis algorithms as well as fingerprint identification, and send CCTV and drone footage directly to the Ministry of Migration and Asylum.[769] The Ministry never refers to these algorithms or fingerprints as biometrics in official documents. BIRN's investigation determined that proper safeguards were not put in place for the systems prior to their rollout (if such a system can even be safeguarded, given the incredible imbalance of power), with the Greek government not appointing a Data Protection Officer or facilitating Data Protection Impact Assessments for either system, despite both being requirements under the EU's GDPR. In March 2022, a number of organisations from Greece and throughout Europe filed a request for an investigation into the systems with which the Greek DPA, the Hellenic Data Protection Authority, complied.[770] However, there have been no recent developments in the case and the DPA has not released any additional information.

One of the investigating NGOs, Greek organisation Homo Digitalis, previously also raised concerns about the Hellenic Coast Guards' intentions to procure social media monitoring systems that would be used to track asylum seekers' activities, as well as to obtain access to their information, including private communications, images, videos and posts.[771] The extent of the systems being put in place by the Greek authorities to monitor asylum seekers seriously infringes upon the human rights and liberties that are guaranteed to communities on the move by a number of international declarations. These deeply-invasive surveillance structures pose a grave threat and can lead to the establishment of a dangerous precedent that could possibly encourage other countries to follow suit. Illegal and dehumanising border practices have already been documented in other EU countries such as Hungary[772] and Croatia,[773] which could be potential future points for the deployment of biometric mass surveillance technologies. This would contribute to the ongoing securitisation of border protection and criminalisation of migration. Such an example also emphasises why it is so important that our definition of biometric mass surveillance include arbitrarily-targeted surveillance, such as against people on the move.

In 2022, a letter to EU decision-makers spearheaded by a group of civil society organisations, including Access Now, European Digital Rights (EDRi), the Platform for International Cooperation on Undocumented

Migrants (PICUM), and the Refugee Law Lab advocated for stronger guarantees within the AI Act when it comes to protections for communities who are pushed to the margins, as well as people on the move, in the context of high-risk AI systems.[774] The letter was signed by 42 organisations and details the ways in which these communities are at a higher risk of being targeted and impacted by these systems. The appeal specifically mentions emerging technologies that are being tested at border crossings, such as remote biometric identification (RBI), emotion recognition, biometric categorisation and automated risk assessments.

Signalling a significant win in several regards, in early May 2023, two committees of the European Parliament voted to endorse protections in the AI Act that would ban several uses of emotion recognition technologies (including law enforcement and migration), biometric categorisation, remote biometric identification in publicly-accessible spaces, and predictive policing systems.[775] Although the move was embraced by many civil society organisations across Europe, it was equally pointed out that there is still a long way to go when it comes to predictive systems. For instance, predictive analytics systems which are not addressed in the Parliament's draft text are nevertheless a key component in how police track and obstruct migration movements. Furthermore, as the EU law section of this book notes, the European Parliament intends to ban RBI in public spaces — but this does not seem to include border crossings, detention centres or camps.

FACEBOOK FOR PALESTINIANS: ISRAEL'S DRACONIAN USE OF BIOMETRIC SURVEILLANCE

Israel's over-policing of Palestinian residents has been steadily increasing over the decades, with biometric surveillance systems constituting a significant part of this. The Israeli government first started using facial recognition software on Palestinians in 1999 to monitor those with working visas coming into the territory.[776] Israel controls all entry and exit points in the West Bank, and this control is effectively streamlined through the use of a comprehensive network of CCTV and databases that include biometric information of Palestinian individuals.[777] Such a set-up perfectly illustrates how software, hardware and databases fit together into a system of punishment and oppression. The Palestinian people's right to movement and right to privacy are grossly violated by these practices, which treat them like walkingbarcodes, and should serve as a stark reminder of the extent of misuses that mass biometric surveillance can bring to communities.

Israel's latest development has been investigated in Amnesty International's 2023 report "Automated Apartheid", which focuses on examining the system nicknamed "Red Wolf".[778] This sophisticated BMS system connects Palestinian faces with pre-existing personal data stored in government and military databases. It also allows Israeli soldiers to train the system by connecting civilians' faces with IDs until the system starts automatically recognising individuals and checking previously collected information in order to assess if they can pass through military checkpoints or if they

should be detained and arrested. All of this, of course, is done without the consent of Palestinian individuals, nor are they notified about the ways in which their personal data are being stored and used, or for how long. The capabilities of this system are still not fully comprehensible to outside researchers or even to the Palestinian people who are subject to it. Amnesty International also identified Hikvision and Dutch-based TKH Security as vendors of much of the surveillance tech used in the country.[779]

Aside from using biometric surveillance systems like facial recognition, Israel is also deeply involved in creating them. AnyVision Interactive Technologies is an Israeli start-up technology company which creates and distributes facial recognition systems with wide-ranging capabilities for biometric mass surveillance. The company has claimed that their software is easily connected to any camera and easily accessible with limited computing skills or capacities.[780] The company has also been linked to top-secret projects that are being facilitated by the Israeli army and deal with checkpoint monitoring of Palestinian people. However, information has come to light that their software was being used inside the West Bank to constantly observe residents of the territory.[781]

The Israeli government has worked on integrating their databases of Palestinian residents' biometric data, and has equipped military forces with phones that have facial recognition technology. The smartphones are able to access the databases through face scans, which allow soldiers to immediately detain or harass Palestinians trying to cross checkpoints or even within the confines of the West Bank. The system is known as "Blue Wolf", and is an extension of the Wolf Pack database in which all private information is initially stored. Soldiers reportedly refer to it as the "Facebook for Palestinians".[782] For a use case so egregious, Suresh and Guttag's taxonomy of harms is arguably of limited use: clearly, even the most technically "perfect" system would do nothing to mitigate the extent to which Palestinians are being routinely controlled and oppressed in ways that are facilitated by biometric mass surveillance tools.

BETWEEN A ROCK AND A HARD PLACE: CENTRAL AMERICA AND THE US' SOUTHERN BORDER

The *non-refoulement* principle is a fundamental aspect of the international migration legal system, which is unfortunately being violated through the pushback, detention and deportation of asylum seekers to third countries, often labelled with the misnomers "safe third countries" or "first countries of asylum".[783] In recent decades, there has been a growing global trend towards externalisation, offshoring and outsourcing of asylum processing to neighbouring and even distant countries. This approach is an attempt to prevent asylum seekers from ever reaching the state border in the first place.[784] As this section has already noted, this has been seen at EU and US borders.

The unfettered pushback in maritime interceptions, along with the possibility of detainment in Guantanamo Bay or deportation to distant Latin countries, has led to asylum seekers trying new landlocked migratory routes. This was clearly demonstrated in 2013, when Mexico (the country of origin of many US immigrants) became a transit country, and one quarter of a million migrants were apprehended at the US-Mexico border. In the last

decade, the US has heavily invested in outsourcing enforcement operations dealing with people on the move, all with the goal of preventing them from ever reaching the Mexico-US border. For instance, since 2020, Panama has detained many trans-continental asylum seekers, including 2,000 Haitians in its southern Darien province.[785] Panama's migration enforcement apparatus receives significant support from the US Department of Homeland Security. The United States has signed "safe third country" or so-called Asylum Cooperative Agreements (ACA) with Mexico and all three Northern Triangle countries (El Salvador, Guatemala and Honduras).[786]

In addition to outsourcing enforcement operations, the exchange of biometric and other personal data of migrants is another element of the vast collaboration framework designed to physically prevent migrants from reaching the US border. The United States signed non-binding memorandums with Mexico in 2017,[787] and the Northern Triangle countries in 2019,[788] agreeing to share biometric data of people on the move as part of the International Biometric Information Sharing Program (IBIS).[789]

However, there is a lack of accountability for all states and actors involved due to the absence of transparency from authorities, the opaque nature of operations in the field, and the vague language and non-binding nature of the agreements.[790] This makes it difficult, if not impossible, to conduct independent assessments of the human rights impact (although the resulting human suffering is all too visible). Watchdog organisations have proposed the introduction of safeguards to protect migrants' human rights. These would include adopting data protection laws in all relevant countries; prohibiting mass profiling, predictive analyses and intrusive geolocation tracking; limiting access to personal data; ensuring special protection of children; requiring informed consent for biometric data processing; and ensuring the enforcement of data protection rights (in particular of access, rectification, deletion and objection).[791]

Foreign data-sharing has become deeply embedded in US immigration enforcement, resulting in numerous due process and civil rights violations. Unverifiable information from foreign police forces is shared through a network of data systems and made available to US Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). While CBP agents screen people at the US border, ICE agents use the provided information as a basis for detention and/or deportation.[792] However, documented case studies have shown that serious problems exist

with the accuracy of this data. The data are provided by foreign police forces that have been reported by the US administration to regularly violate human rights and liberties and engage in corrupt behaviour. For example, one asylum seeker was fleeing his country because police officers had intimidated him and asked him to give false witness testimony, only to find himself in detention due to malicious data about him that was provided by the same police force.[793] When deciding on migration cases, the US administration and judiciary frequently utilise information on apparent gang association, despite such information lacking any discernible means of establishing its validity or basis. The National Immigrant Justice Center (NIJC) has provided legal counsel to more than one hundred separated parents and their children. Most often, individuals are labelled as gang affiliated without due process or supporting evidence.[794]

The enforcement of US migration policy has had a clear detrimental impact on the rights and freedoms of people on the move. The unfettered pushback in maritime migratory routes has redirected people on the move to landlocked paths, increasing migratory pressure on the US-Mexico border and prompting the US to invest heavily in Northern Triangle countries' capabilities to find, detain and deport migrants. This has forced migrants to embark on ever-more dangerous routes that are beyond the reach of US-funded capabilities of local authorities. One such route is the notorious Darien Gap — a roadless[795] and lawless area of mountainous rainforest in Colombia and Panama,[796] where "robbery, rape and human trafficking are as dangerous as wild animals, insects and a lack of clean water".[797]

It is difficult to calculate the ultimate human cost of US immigration policy.[798] This vast enterprise, whose sole goal is keeping people on the move off the US border, relies on externalisation and outsourcing of enforcement operations to Central American countries, which would not be possible without the transborder exchange of people's personal data, biometrics included. While such data are not reliable (especially gang affiliation information), they are taken at face value and determine the fate of migrants and their families. Negative impacts on human rights are overlooked by both the US and Central American countries — the first content with expanding the reach of its enforcement away from the border through externalisation and outsourcing, the latter eager to maintain and expand US investments in the externalising and outsourcing of the processing of asylum seekers.


овары для дома
99
АКЦИЯ
merci

TECHNOSOLUTIONISM GOES PRIVATE: USES OF BIOMETRICS IN THE PRIVATE SECTOR

This area of interest is slightly different from the cases already observed in this book, where states were ultimately responsible for the biometric mass surveillance practices. In the previous cases, companies played everything from a facilitating role to an encouraging or even instigating role, but here, they take centre stage. Traditionally, private entities have not been responsible like governments for the well-being of citizens and residents. Moreover, they are motivated by profit, and therefore work in the interest of generating it — as the technical section of this book has clearly shown. Yet companies are not devoid of all responsibility and should also be able to account for the technologies they are implementing. In fact, with the introduction of the UN's Guiding Principles on Business and Human Rights, more and more legal systems are considering or implementing clear human rights obligations on companies.[799] This segment looks at three specific aspects of the private, for-profit implementation of biometric surveillance systems that are on the rise worldwide.

SMILING FACES AND CONTROLLED SPACES: BIOMETRICS IN RETAIL

At first glance, the use of facial recognition and other biometric technology might evoke images of shoppers paying for their purchases with selfies or their fingerprint — which is risky enough, as a later case study will touch on. But the ways in which they can be tracked as they navigate through stores is a more pressing and less studied issue. CCTV and other "traditional" surveillance systems have been in use in the retail industry for a long time . However, certain retail chains have recently been upgrading their systems to include the use of facial recognition technologies, which are more intrusive and rely on the use of biometric data.

The main justification for the use of surveillance in shops tends to be security reasons. Yet we would argue that there is no sufficient justification for collecting and retaining personal data in order to approach this issue, given the availability of less-intrusive alternatives. This is especially true in instances where customers are not aware that they are being surveilled when they enter stores, such as in the case of three large Australian retail chains.[800]

After a consumer group revealed the secretive use of facial recognition technology to surveil shoppers by Australian retail giants Bunnings, Kmart and The Good Guys, a wider conversation about the use and retention of

personal data by supermarket giants was sparked. CHOICE, the consumer advocacy group, surveyed a number of Australia's leading retailers and found that only those three collect and store biometric data through their facial recognition software. The group has also pointed out that the physical signs posted up at the stores, which are supposed to inform customers that they will be subject to facial recognition technology (FRT) upon entering the stores, are too small, easy to miss, and overall negligible.[801]

Both of these practices would account for potential violations of Australia's Privacy Act, which stipulates a proportionate collection of sensitive data, including biometrics. The Act also notes that the data collection must be suitable for business purposes, which would require a more detailed explanation from the companies using these technologies. In line with these observations, CHOICE has asked the Office of the Australian Information Commissioner (OAIC) to investigate the retailers' practices concerning the use of facial recognition and biometric data collection.[802] As soon as the OAIC announced its probe into the retailers, all three companies suspended their use of the technology.[803] As of February 2023, the OAIC has said that their investigation into Kmart and Bunnings will be completed by July.[804] As of current, there have been no updates on the case.

The Commissioner's Office also revealed that its investigation into The Good Guys appliance chain has been dropped, since the company stated that it would be halting its use of FRT, initially while the investigation was being undertaken, which then became indefinitely.[805] The 2022 complaint filed by CHOICE for the retailers' use of biometric data leaned heavily on a previous case concerning convenience superstore 7-Eleven, which used FRT on their in-store tablets in order to rate customer satisfaction. The company tried to argue that their use and collection of facial images did not constitute a breach of the Privacy Act, since they claimed that the data were not being used to identify and monitor individuals. However, the practice was discontinued following the OAIC investigation, which stipulated that there was no evidence that biometric data was necessary for evaluating customers' in-store experience, and 7-Eleven was obligated to delete all of the previously collected customer data.[806]

In a similar case, Amazon, who in 2021 was lauded by some for apparently stopping police from using their facial recognition software, has been involved in two cases of deceitful biometric data collection at their "Go" physical stores in New York City.[807] It was alleged by the plaintiffs in the

subsequent cases that the store did not adequately display a sign at the entrance to notify customers that upon entry their biometric data was collected.[808]

Other cases elsewhere also indicate that FRT is being used for additional monitoring of customers, such as systems that prevent customers from scanning the wrong thing at self-checkout stations.[809] Additionally, concerns about hyper-personalised pricing have also surfaced with the introduction of such technologies, since there is no feasible way to know where retail stores decide to draw the line when they have access to such sensitive consumer information.[810] This would mean that stores would be able to target specific customers who are inclined to use store apps to buy their products, and price fix based on the collected information. Although hyper-personalisation practices have been active for over a decade,[811] the introduction of FRT into the mix stands to create a new area of concern, especially if these practices are overused and under-regulated.[812] The kind of pervasive online tracking, for example across social media platforms, that digital rights groups have fought against for years, are being brought into offline spaces thanks to such uses of biometric surveillance technologies.

Therefore, transparency is a key tool in ensuring that misuses of such practices do not go unchecked (or happen at all), and can incentivise companies to be more mindful towards their customers' data. This is especially true for products that gather sensitive data, such as Amazon's Alexa, which collects and stores voice data, and other products reliant on biometric features and sensors retention.[813]

Using biometric data to identify shoppers poses a number of potential harms — for one thing, misidentification is sure to occur, and there have already been prominent cases involving huge tech giants such as Apple.[814] Apple was accused of misidentifying a shoplifter through their in-store facial recognition software and filing a police complaint against a teenager who never entered the store nor even the state in which the incident had occurred.

The negligence present in the case points to deeper rooted systemic problems within which such systems operate. According to the filed lawsuit, Apple and its security contractor, Security Industry Specialists (SIS), consciously misidentified an individual accused of shoplifting in one of their stores through the mismanagement of their surveillance system. It was uncovered that human error deferred the arrest of the real perpetrator, because he was

carrying the accused teenager's stolen driving permit. Instead, the decision was made to connect surveillance footage to the permit without additional checks, and subsequently the police made no further effort to validate the suspect's identity.[815] The only feature connecting the two men was their race.

Other countries and jurisdictions have also seen retailers rush to implement facial recognition and other forms of biometric surveillance in their shops. In the UK, the Co-op supermarket came under fire for using facial recognition to identify and obstruct shoppers who had been placed on a watchlist by other retailers — with no evidence or independent assessment of whether the people on the watchlists had committed or attempted to commit any crime.[816] In Europe, Dutch facial recognition company VisionLabs is one of many that offer the use of biometric systems to profile shoppers as they move around a store — including through the path that they take, the items that seem to interest them, their emotions, and more.[817]

Pressure in the US has been mounting on large retailers to halt the use of facial recognition in their stores. Fight for the Future, a US-based collective of activists, started a campaign to ban facial recognition in stores, and allows customers to view which retailers use facial recognition technology in their stores as well as those who have made a pledge to refrain.[818] Private companies are obligated to align their use of surveillance systems with local laws, and may therefore be incited to change their practices by concerns and complaints coming from consumer groups and public officials. The amount of oversight and potential room for influence does depend on the specific country in which the companies operate and can therefore lead to diverging practices.[819]

PRIVATE TECHNOLOGY IN PUBLIC SERVICE

Previously in the book, we have touched upon how governments opt to utilise biometric surveillance technologies for what they claim are national, border and port security reasons. But another avenue through which governments have started cosying up to biometrics relates to socio-economic development. Around the world, small and large countries are finding new ways to incorporate residents' sensitive data into everyday practices.

It is important to note that none of these advances are risk-free. Governments need to seriously consider the privacy threats involved when working on developing and adjusting new technologies to their and their residents' needs, as well as carefully evaluate third party vendors with which to work on their implementation.

The security of residents' personal data can play an influential role in governments' decisions to use biometric technologies in everyday life. Ensuring residents' interactions and satisfaction with public e-services has become increasingly challenging for governments, especially in the face of the COVID-19 pandemic, which has had a significant impact on in-person sectors — the majority of government services — since 2020. As a result, governments have seemed to shift focus on finding new ways to expand the digital frontiers in an effort to deal with questions of residents' personal information security, but in the process have seemingly overlooked privacy concerns. Access to life insurance policies, medical information, finance management and secure online communication with public services staff

all require some form of verification. Although passwords are still the most widespread form of identity authentication, many companies increasingly offer purportedly more advanced tech "solutions". Obviously, this poses a number of challenges, since e-services for the most part continue to be developed by third-party vendors. Some service providers, such as banks, opt for integrating biometric technologies used by major tech companies like Apple and Samsung, which in the past have been criticised for lacking privacy by design models.

In Asia, biometrics are becoming an increasing part of everyday government services operations. Thailand has already added facial recognition to bolster their authentication of new banking customers by integrating the government-initiated National Digital ID platform (NDID).[820] The NDID is a privately-owned digital ID services company that claims to simplify citizen verification processes for companies and services throughout various sectors such as banking operations, healthcare, taxpaying and insurance.[821] In early 2022, the NDID partnered with Mastercard to offer their verification services outside the country, which would allow them to expand their list of potential client companies internationally.[822] The way in which the NDID was able to grow to this extent in a relatively short amount of time was credited to a regulatory sandbox which allowed them to test out their services in real-time on residents, without worrying about violating privacy laws. The sandbox principle exempts such services from regulatory compliance and allows the company a carte blanche to collect evidence on the efficacies of their technology. While in Thailand's case this experiment reportedly helped the country grow its digital GDP, which is expected to amount to a third of the country's overall GDP in the next five years,[823] the stakes are too high not to consider the potential downsides of such integrated systems which contain residents' biometric data.

In Russia, the Unified Biometric System (UBS) is a state-sponsored and state-developed system which allows Russian residents to access and use a number of services across the country.[824] The system was developed in collaboration with the Bank of Russia and Rostelecom, Russia's biggest telecommunications service provider, and collects individuals' biometric identifiers such as voice and face prints. The UBS has become a central part of all the biometric identification tech distributed among Russian-based banks and other businesses since 2018. The personal data collected by banks in the country is done through a twofold process — first the bank collects individuals' biometric data for their own security purposes, and

then the data is collected to pass onto the UBS.[825] Although the collection of biometrics for the UBS is still on a voluntary basis, reports have been released that the government has called for the system to be integrated into secure spaces in the country such as defence and nuclear facilities.[826] However, in 2022, Russia's lower parliament house adopted a bill which would mandate banks to submit clients' biometric data to the government without clients' prior consent.[827] The mass centralisation of biometric data in Russia has been linked by privacy experts to an organised push to control as much information on citizens as possible, since banks were ordered to hand over clients' biometric data by the states' security services.[828]

The mass centralisation of personal data systems can pose a number of threats to individuals' privacy, from breaches to misuse of data, and the risks can grow increasingly with biometrics in the mix.

THE BILLION-FACE DATABASE: CLEARVIEW AI

The private sector has been at the forefront of expanding the use of facial recognition and other biometric technology across the world, which has a growing impact on the interests and rights of residents. Private companies function both as suppliers (developers) and purchasers of biometric technology. However, the laws regulating the use of facial recognition and other biometric surveillance are often not sufficient to deal with the scale of the harms entailed, as the Legal section of this book has emphasised.

Consequently, private companies frequently develop products, business plans and marketing strategies without sufficiently considering negative externalities such as discrimination, invasion of privacy and the risks to other human rights. These issues are often left to the general public to create public pressure for the introduction of government regulations, or for privacy activists and human rights defenders who engage in strategic litigation to curb the use of such technologies. The case of Clearview AI exemplifies this situation — with abuses of biometric data so numerous that several other chapters of this book have already explored the issue across various jurisdictions.

Clearview AI has gained notoriety for its facial recognition service, which relies on a face biometrics database constructed by scraping personal photos published online, primarily from social networks.[829] The core business model and the tool itself are built on profoundly illegitimate processing of

personal data, deemed entirely unlawful under the GDPR. In the European Union, Clearview AI has faced a series of fines resulting from strategic litigation by privacy activists and *ex officio* actions taken by European Data Protection Authorities (DPAs). The DPAs of three EU Member States have issued €20 million fines to Clearview AI: Italy (March 2022),[830] Greece (July 2022),[831] and France (October 2022).[832] Even before these decisions by EU DPAs, the UK DPA ICO issued the company a £7.5 million fine (December 2021).[833] Just recently (May 2023), the French DPA issued yet another fine of €5.2 million for not complying with orders issued with the first fine.[834] The Austrian DPA also deemed the company's practices illegal, but no fine was issued.[835]

Until 2020, Clearview AI sold its services to both private companies and public authorities. However, this business plan was struck down by a lawsuit filed by the ACLU, leading to a ban on the sale of their services to private companies in the United States.[836] Nevertheless, the company continues to provide its services to law enforcement agencies, contributing to the ongoing debate on the use of facial recognition and regulation in the US, particularly in relation to the ways in which the use of these systems entrench and exacerbate racist policing. The technical aspects regarding the accuracy of facial recognition technology are extensively discussed in the Technology chapter of this book, while the adverse societal effects arising from its use are presented in the case study examining the implementation of facial recognition by the NYPD.

Apart from the banking and retail sectors, it is law enforcement, including the national security apparatus, which is driving the demand for facial recognition and other biometric surveillance capabilities and tools. Clearview AI has garnered public attention due to its highly questionable data processing practices and its popularity among US police departments. The general public tend to become aware of facial recognition technology use only when it directly impacts policing procedures on the ground, which they themselves are witness or subject to. In contrast, many companies that supply biometric surveillance technology to the broader law enforcement community are characterised by opacity, operate under the public radar and without public scrutiny. Research shows that the US government awarded $76 million worth of unclassified facial recognition-related contracts in the last two decades.[837] However, the worth of classified contracts awarded by the federal law enforcement agencies or the military is expected to be much higher.

While the largest biometrics companies and technology suppliers are located worldwide, it appears that, perhaps due to the lack of federal regulation discussed in the previous chapter, American companies are consistently willing to "move fast and break things". This approach to unbridled development and selling of facial recognition tools and services is recently being questioned by private companies themselves. Some of them have even purportedly halted the development or limited the sale of such tools. For example, Microsoft decided to limit its suite of artificial intelligence offerings and discontinued its facial analysis tools that are able to detect a person's emotional state due to inaccuracies and discriminatory applications — although as chapter one notes, there are concerns about how genuine and effective this moratorium actually is.

EYES, EARS AND AWARENESS: CONTROL OF PUBLIC SPACES

The increasing normalisation of the constant surveillance of public spaces raises a number of concerns about privacy and civil liberties. Residents have a right to privacy and should not feel like they are constantly being watched or their every move is being monitored. Massive football and other sports stadiums have established themselves as one of the most convenient testing grounds for new surveillance technologies all around the world. The reasoning for this is that governments understood that major sporting events are a very convenient way to usher in and justify the mass use of surveillance technologies, as well as try them out before further deployment in society. This is why the majority of cases that involve public space surveillance, most recently the 2022 FIFA World Cup in Qatar[838] and the 2024 France Olympics,[839] are always steeped in technosolutionist controversy. Conversely, it is worth mentioning that the facial recognition surveillance of stadium goers also involves a financial aspect, as it allows companies to protect their interests. Such was the case of FIFA cracking down on fans for wearing a certain colour at the 2010 World Cup, because the organisation suspected that they were carrying out a campaign for a brand that sought to advertise at the game but was not an official FIFA sponsor.[840] With 15,000 cameras deployed in Qatar for the 2022 World Cup, the Chief Technology Officer of the company handling the surveillance infrastructure at the event called the system "the eyes, ears and awareness of all stadiums at the same time".[841] This intrusion on privacy fosters a culture of fear and inhibits personal freedoms, ultimately undermining the democratic fabric of society.

VIVE LA SURVEILLANCE! — THE 2024 FRANCE OLYMPIC GAMES

National security is often a shorthand for government-led deployment of facial recognition technologies, especially in cases such as parades, festivals or sporting events. It then comes as no surprise that the Olympic Games are a major point of contention when governments try to balance security and privacy. In *Security Games: Surveillance and Control at Mega-Events,* Colin Bennett and Kevin Haggerty argue that these mega-events provide a breeding ground for experimentation with monitoring and surveillance of public spaces, and require little to no explanations of the safeguards which should be put in place beforehand. They also note that "[s]ecurity has become an integral part of the Olympic ritual".[842]

Notably, one of the main incentives for increasing the securitisation of mega-events was the 9/11 attacks, which have given governments blanket authority to experiment with invasive technologies. As discussed in our overview of the use of surveillance in the context of national security, an added layer is present in the organisation of major events, especially those with an international character that attract a major audience, such as the World Cup or the Olympics. These events have social, economic and national importance for the host country, and are therefore usually a stage to display the country's capabilities to control and facilitate these events. Unfortunately, the main area of competition at these events has become the increased surveillance of the public.

At the centre of one of the most privacy-regulated parts of the world, the EU, a long-brewing discussion has surrounded the securitisation of the

Olympic Games. France, which will be host to the 2024 Summer Olympics and Paralympics, has had a rocky road coming to terms with how it wants to approach the issue of surveillance and security in light of next year's ceremonies. In November 2022, the French government vowed not to use facial recognition technology, citing it as a "red line" in terms of privacy violations.[843] However, in March 2023, the Parliament approved Article 7 of the Olympic Games law, which stipulates the use of automated behavioural surveillance of public spaces for the duration of sporting, recreational or cultural events..The government argued that this did not include capabilities for uniquely identifying a person.[844]

Despite strong opposition from MEPs and civil society organisations,[845] the French government managed to push the bill through. It was helped by the fact that the controversial retirement reform was the focus of attention at that time, and left no space for public debate to raise awareness about biometric surveillance. Privacy and civil rights advocates have pointed out that this sets a dangerous precedent not only in France, but in Europe more broadly. They have also scrutinised the supposed remarks by the government that the automated video surveillance technology does not amount to or in any way utilise biometrics, citing that this is a clear misconception and a reinterpretation/misuse of legal concepts.[846] The automated surveillance technology is supposed to aid police authorities in monitoring and flagging "suspicious behaviour" at the event. At the time of writing, the government has not yet released a decree which would define the given flagged behaviours, but we can conclude that targeted suspicious behaviours would be common ones such as walking the wrong way in a crowd, lying down in the street, running, etc. The real-time surveillance software is capable of detecting items and behaviour that can potentially be flagged as risk-prone by authorities.[847]

The development of surveillance tech employed for national security purposes at major events has been steadily increasing both in quantity and sophistication. By some estimates, while budgets for securing the Olympics in 2000 were in the millions, following the 9/11 attacks those numbers grew into the billions.[848] However, when analysing the many areas in which surveillance technology deployed at the Olympic Games has been used in the past, we notably find reports of over-policing of impoverished, minoritised and racialised communities documented during the 2016 Rio Olympics.[849] The use of the technology allows authorities to decide who can

be present where and in what manner. Therefore, the potential for misuse of such technology during, but also after the events, lacks critical scrutiny.

The French Olympics law is another example of governments utilising major events to push a security agenda and promote economic interests within the country. It also plays into the evolving desires of France's large algorithmic video surveillance industry to regulate the use of these technologies, allowing its players to increase their production and test and sell their systems to the state.[850]

In May 2023, the French Constitutional Court approved the bill and supported the government's rollout of algorithmic processing systems. The experimentation phase will last until April 2025, long after the Olympic Games comes to an end.[851] The other major issue is that, according to the French government, biometric data are only related to facial recognition, which neglects behavioural analysis as part of the processing of biometric data. Therefore, the ban put into place by the Constitutional Court can be interpreted as a purely symbolic one, without much practical consequence from a legal perspective.

This case highlights the importance of legal frameworks ensuring broad definitions of biometric data. Otherwise, there is a very real risk that governments will be incentivised to search for loopholes and draw arbitrary distinctions between practices that they accept are too harmful, and those that they argue are acceptable because they do not fit the full technical definition.

THE CROWN JEWEL OF CONTROL — THE UK CORONATION

In the last decade, the United Kingdom (UK) has cemented itself as one of the most prolific countries in Europe when it comes to deploying biometric mass surveillance systems in public spaces. Some of the most high-profile examples include a secretive partnership between London's metropolitan police (the Met) and property developers around the Kings Cross travel hub from 2016 to 2018;[852] the surveillance of Christmas shoppers in 2017 and peaceful protesters in 2018, both by South Wales police;[853] the fine given to a man who covered his face to avoid live facial recognition (LFR) in 2019;[854] and the targeting by the Met police of primarily Black communities celebrating the Notting Hill carnival (an annual celebration of London's Afro-Caribbean communities) in 2017.[855] This is particularly alarming because as recently as 2023, an independent study found the Met police to still be "institutionally racist",[856] decades after systemic discrimination in the Met was first brought to public attention.

These worrying examples, and numerous others, have led to non-governmental organisations (NGOs) such as Liberty and Big Brother Watch vocally contesting the UK's quick recourse to facial recognition as an alleged easy solution to practically any social or criminal issue.[857] They have pointed out the significant threats to racial justice, with many of the deployments happening without any consideration of the bias of facial recognition systems, nor the discriminatory structures within which they are deployed, leading to the over-targeting of racialised communities.

These UK police pilots and deployments of biometric surveillance have also been interrogated by several leading academics, including a landmark study by Professor Pete Fussey and Dr Daragh Murray in 2019.[858] Fussey and Murray's research was the first independent study into the use of facial recognition by UK police, and found serious operational failings, a major lack of oversight, and many practices that would likely be deemed unlawful if challenged in court. Other leading academics, such as Professor Lorna McGregor of the Human Rights, Big Data and Technology (HRBDT) Project, along with Professor Fussey, have used their interdisciplinary human rights lens to contest these reckless deployments of facial recognition by the UK state.[859]

It is not just government authorities that have been responsible for the UK's boom in biometrics. Supermarkets, in particular, have been quick to experiment with these technologies. Facial recognition was notably used to enforce no-entry policies by the Co-op supermarket chain.[860] Moreover, a wide range of services (including major supermarket chains like Sainsburys and Tesco, as well as post offices) piloted biometric-based systems for verifying the age of shoppers to determine whether they could buy age-restricted products.[861] Similar practices are explored earlier in this chapter in the Australia case study.

More broadly, the UK biometric age-assurance company Yoti has partnered with large online platforms like Instagram,[862] despite open questions about the compatibility of their practices with human rights rules. As NGO Privacy International has highlighted, the rapid uptake of Yoti and other similar services has been underpinned by a specific goal by the UK government to foster a globally-leading "digital identity" industry.[863]

The Biometrics Institute, a UK-based association, has also attracted attention for pushing the vested interests of the biometrics industry, whilst presenting itself as a non-partisan group.[864] In fact, the biometrics industry is so central to the UK's economy that it was estimated to be worth over half a billion pounds in 2022.[865] It is clear, therefore, that along with social control and technosolutionism, the UK's prolific use of facial recognition and other biometric systems has also been driven by economic interests. Specifically, there is a state-sponsored desire to have the most extensive market for biometrics in the world — an aspiration that, based on the research described in the Legal chapter of this book, is clearly matched by the government of China. Whilst not every use of biometrics is automatically

mass surveillance, these steps can create the underlying conditions and infrastructures to allow biometric mass surveillance practices to flourish.

In particular, it appears that the widespread commercial use of biometric systems — coupled with the UK's extensive underlying CCTV camera network (the largest in Europe, with one camera per every 13 people)[866] — have contributed to an unconscious normalisation of biometric mass surveillance in the UK. Such practices can make it even harder for people to be alert to what is happening, and less aware of why it can pose such a risk to their rights and freedoms.

In the context of such careless experiments, profit-driven expansions, and a belief in technological surveillance as the solution to practically any problem, the coronation of King Charles has demonstrated exactly why the UK's use of facial recognition in public spaces is so concerning. Notably, the use of facial recognition systems has been intertwined with the UK's disproportionate and heavy-handed treatment of both celebrations and protests relating to the coronation, in a way that shows the power of these systems to control and suppress the right to enjoyment of public spaces.

On 6 May 2023, the coronation of King Charles III was an event that emphasised the polarised attitudes of UK citizens and residents towards the monarchy. In the run-up to the event, many people and communities were preparing for street parties and other forms of celebration. Many others were organising protests and other forms of lawful dissent. Several of these protests were driven by criticisms of the institution of the monarchy broadly, as well as the specific actions of the UK's royal family.[867] Many people also criticised the large public spending on the day of the coronation at a time when millions of UK children cannot afford to eat three meals a day.[868]

A few days before the coronation, the Met police announced that they would be pursuing their largest ever deployment of live facial recognition (LFR) as part of policing the event, with Professor Fussey noting that this deployment is "probably the largest ever seen in Europe".[869] The Met police were quoted as seeing the coronation as an opportunity to use facial recognition "to pick up the people who are wanted for an offence or who have a warrant out against their name".[870]

The use of celebrations and protests as an opportunity for police to seek persons wanted for reasons unrelated to those activities suggests that police efforts are not focused on upholding the rights of people attending

to enjoy the public spaces. Rather, these legitimate, lawful activities are seen as an opportunity to achieve other policing goals. This suggests that police resources and attention were not focused on keeping the celebrants and protesters safe. The right to protest has been repeatedly upheld by the European Court of Human Rights and it is the duty of the state to respect and secure that right.[871]

Worse still, biometric surveillance technologies have been widely recognised to create a chilling effect that can deter people from exercising their rights and freedoms, in particular the rights to assembly and association.[872] Despite this, the Met police are deliberately employing them to police protests. It is possible that the Met police may even have seen the use of live facial recognition, an obvious form of biometric mass surveillance, as a way to pre-emptively discourage people from enjoying their right to protest. Evidence for this interpretation can be seen in heavy-handed social media posts by the Met police, which warned people against protesting, calling it "disruption" and strongly hinting that protesters would be arrested.[873] These posts were widely condemned on social media for being repressive and authoritarian. The use of LFR is thus deeply tied up in these broader policing issues.

Moreover, whilst *prima facie* it may seem legitimate for the police to seek wanted persons, there is the additional factor that on the same day that the Met announced its use of LFR for the coronation, the UK's new Public Order Act (2023) came into force.[874] Building on the Police, Crime, Sentencing and Courts Act (2022),[875] these laws have been strongly criticised for criminalising certain forms of protest, and doing so in a way that is vague enough to potentially discourage a significant number of people from participating in protest or other lawful dissent — including because it could even allow police to arrest protesters who link their arms together.[876] The UK Home Office allegedly wrote to one protest group, Republic, shortly before the coronation, to warn them that these new laws were designed to discourage groups like theirs from protesting at large-scale public events or taking other "disruptive" actions.[877]

These new laws would give the Met police the power to arrest many of the day's protesters, criminalising their freedom of speech to criticise the coronation as well as their freedom of assembly to join with others to make this point. In turn, the LFR system would give them the ability to locate and identify protesters, which would make any reasonable person feel less comfortable and safe to attempt to protest, knowing how easily they could

be tracked in real-time. These actions by the Met police further cement the repressive power of the LFR deployment and the role of biometric mass surveillance in persecuting people trying to enjoy their fundamental right to protest.

Lastly, the issues surrounding UK police deployments of facial recognition systems raised at the beginning of this section, such as the lack of transparency and disregard for the high risk of discrimination, have never been formally resolved. This further compounds the harms, and shows the flagrant disregard for human rights by the Met police in deciding to use LFR at the coronation. Following the live facial recognition deployment at the coronation, the UK's Biometrics and Surveillance Camera Commissioner, Fraser Samson, warned that "oversight and regulation in this increasingly important area of public life is incomplete, inconsistent and incoherent".[878]

Overall, this case paints a picture of biometric mass surveillance as one tool in the UK state's wider arsenal of techniques to control and shape public spaces. LFR has been used, particularly by the London Metropolitan police, to punish normal behaviours like covering your face in public, to criminalise democratic actions like protest, and to further target Black and other racialised communities. Building on the taken-for-grantedness of public surveillance thanks to the UK's vast CCTV camera network, UK police have largely been able to quell public opposition to biometric mass surveillance, despite the important efforts of NGOs and academics.

Against this backdrop, supermarkets and other private entities have been quick to pilot the use of biometric or biometric-based data for other functions, such as verifying shoppers' ages. Along with prolific police uses, these commercial uses compound the subconscious normalisation of biometric systems for a wide range of purposes in the UK.

The UK is only increasing its use of people's most sensitive data to control who can and cannot enjoy public spaces, amenities and fundamental rights. At the same time, we can see that the already insufficient legislative safeguards against biometric mass surveillance are increasingly being removed. In particular, Commissioner Samson has warned that the only legally-binding framework in place in the UK specifically for such biometric surveillance practices is about to be abolished, "and there are no provisions for its replacement".[879]

ENDNOTES

1 IBM, "What is Computer Vision?", https://www.ibm.com/topics/computer-vision

2 S. Lewis, "The Racial Bias Built Into Photography", The New York Times, April 25, 2019, https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html

3 V. Joler, M. Pasquinelli, "The Nooscope Manifested: AI as Instrument of Knowledge Extractivism", 2020, https://nooscope.ai/

4 K. Crawford, T. Paglen, "Excavating AI: The Politics of Images in Machine Learning Training Sets", The AI Now Institute, NYU, September 19, 2019, https://excavating.ai

5 R. Mac, "Facebook Apologizes After A.I. Puts 'Primates' Label on Video of Black Men", The New York Times, September 3, 2019, https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html; M. Zhang, "Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software", Forbes, July 1, 2015, https://www.forbes.com/sites/mzhang/2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/

6 J. Vincent, "Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech", The Verge, January 12, 2018, https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai

7 Labeled Faces in the Wild Home, http://vis-www.cs.umass.edu/lfw/

8 G. Bae et al., "DigiFace-1M: 1 Million Digital Face Images for Face Recognition", Winter Conference on Applications of Computer Vision 2023, https://microsoft.github.io/DigiFace1M/

9 European Digital Rights (EDRi), "Remote biometric identification: a technical & legal guide", January 23, 2023, https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/

10 National Human Genome Research Institute, "Fact Sheet: Eugenics and Scientific Racism", https://www.genome.gov/about-genomics/fact-sheets/Eugenics-and-Scientific-Racism

11 L. Lee-Morrison, "Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face", transcript publishing, 2019, pp. 85-87

12 M. Rouse, "Pixel", Techopedia, August 31, 2020, https://www.techopedia.com/definition/24012/pixel

13 L. Lee-Morrison, "Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face", op.cit., p. 67

14 L. Sirovich, M. Kirby, "Low-Dimensional Procedure for the Characterization of Human Faces", Journal of the Optical Society of America. A, Optics and image science 4 (3): 519-24, 1987, DOI:10.1364/JOSAA.4.000519, https://www.researchgate.net/publication/19588504_Low-Dimensional_Procedure_for_

the_Characterization_of_Human_Faces, pp. 520-521

15 Wiktionary, "Eigen", https://en.wiktionary.org/wiki/eigen#German

16 L. Lee-Morrison, "Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face", op.cit., p. 72

17 Ibid., p. 72

18 Source: M. Dussenbery, "On Eigenfaces: Creating ghost-like images from a set of faces.", January 22, 2015, https://mikedusenberry.com/on-eigenfaces

19 M. Turk, A. Pentland, "Eigenfaces for Recognition", Journal of Cognitive Neuroscience 3 (1): 71-86, 1991, https://doi.org/10.1162/jocn.1991.3.1.71, p. 72

20 Ibid., p. 71

21 Ibid., p. 86

22 L. Krahulcova, "Techno solutionism—very few things actually need to be an app.", Digital Rights Watch, March 25, 2021, https://digitalrightswatch.org.au/2021/03/25/technosolutionism/; M. Rouse, "Technodeterminism", Techopedia, November 19, 2012, https://www.techopedia.com/definition/28194/technodeterminism

23 V. Joler, M. Pasquinelli, "The Nooscope Manifested: AI as Instrument of Knowledge Extractivism", 2020, https://nooscope.ai/

24 M. Schaake, "Trade secrets shouldn't shield tech companies' algorithms from oversight", Brookings TechStream, May 4, 2020, https://www.brookings.edu/techstream/trade-secrets-shouldnt-shield-tech-companies-algorithms-from-oversight/

25 Merriam-Webster.com Dictionary, "Biometrics.", Merriam-Webster, https://www.merriam-webster.com/dictionary/biometrics

26 S. Minaee et al., "Biometrics Recognition Using Deep Learning: A Survey", arXiv:1912.00271v3 [cs.CV], https://doi.org/10.48550/arXiv.1912.00271, pp. 1-2

27 V. Joler, M. Pasquinelli, "The Nooscope Manifested: AI as Instrument of Knowledge Extractivism", 2020, https://nooscope.ai/

28 Ibid.

29 Amazon Web Services, "What is a Neural Network?", https://aws.amazon.com/what-is/neural-network/

30 A. Trafton, "Study urges caution when comparing neural networks to the brain", MIT News Office, November 2, 2022, https://news.mit.edu/2022/neural-networks-brain-function-1102

31 Amazon Web Services, "What is a Neural Network?", https://aws.amazon.com/what-is/neural-network/

32 Source: F. van Veen, "The Neural Network Zoo", The Asimov Institute, September 14, 2016, https://www.asimovinstitute.org/neural-network-zoo/

33 IBM, "Convolutional Neural Networks", https://www.ibm.com/topics/convolutional-neural-networks

34 M. Rouse, "RGB Color Model (RGB)", Techopedia, September 19, 2015,

https://www.techopedia.com/definition/5555/rgb-color-model-rgb

35 Y. Gavrilova, "Convolutional Neural Networks for Beginners", SeroKell, August 3, 2021, https://serokell.io/blog/introduction-to-convolutional-neural-networks

36 Ibid.

37 Ibid.

38 IBM, "Convolutional Neural Networks", https://www.ibm.com/topics/convolutional-neural-networks

39 Google Research, "Google Brain", https://research.google/teams/brain/

40 Microsoft Research, "Deep Learning Group", https://www.microsoft.com/en-us/research/group/deep-learning-group/

41 V. Joler, M. Pasquinelli, "The Nooscope Manifested: AI as Instrument of Knowledge Extractivism", 2020, https://nooscope.ai/

42 B. Ammanath, K. Firth-Butterfield, "How deep learning can improve productivity and boost business", World Economic Forum, January 12, 2022, https://www.weforum.org/agenda/2022/01/deep-learning-business-productivity-revenue/

43 When it comes to Serbia, the second version of the Data Protection Impact Assessment for the "Safe City" smart video-surveillance project in Belgrade published by the Ministry of Interior in 2020 contained information about 8100 devices to be procured for the system: fixed and moving pole-mounted street cameras, fixed police vehicle mounted cameras, uniform cameras for police officers and hand-held eLTE terminals. See more at: SHARE Foundation, "Kamere bez upotrebne dozvole / Procena uticaja 2.0", July 31, 2020, https://www.sharefoundation.info/sr/kamere-bez-upotrebne-dozvole-procena-uticaja-2-0/ (in Serbian)

44 B. Ammanath, "Facial Recognition: Here's looking at you", Deloitte AI Institute, 2021, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-facial-recognition.pdf, p. 5

45 J. Cox. J. Koebler, "Ransomware Group Claims Hack of Amazon's Ring", Vice/Motherboard, March 14, 2023, https://www.vice.com/en/article/qjvd9q/ransomware-group-claims-hack-of-amazons-ring

46 J. Kelley, M. Guariglia, "Ring Reveals They Give Videos to Police Without User Consent or a Warrant", EFF, July 15, 2022, https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant

47 Electronic Privacy Information Center (EPIC), "Drones and Aerial Surveillance", https://epic.org/issues/surveillance-oversight/aerial-surveillance/

48 For photo reference see: T. Paglen, "Untitled (Reaper Drone)", Institute of Contemporary Art Boston, 2012, https://www.icaboston.org/art/trevor-paglen/untitled-reaper-drone

49 J. Honovich, "How to Design a Video Surveillance Solution", IPVM, January 4, 2012, https://ipvm.com/reports/how-to-design-video-surveillance-solution

50 X. Fu, "Design of Facial Recognition System Based on Visual Communication Effect", Computational Intelligence and Neuroscience, vol. 2021, Article ID

1539596, 9 pages, 2021, https://doi.org/10.1155/2021/1539596, p. 2

51 X. Fu, "Design of Facial Recognition System Based on Visual Communication Effect", op. cit., p. 3

52 MEP Patrick Breyer, "Expect biometric mass surveillance in Paris in 2024: French Parliament approves automated monitoring of public spaces for 'suspicious behaviour'", Patrick-Breyer.de, March 24, 2023, https://www.patrick-breyer.de/en/expect-biometric-mass-surveillance-in-paris-in-2024-french-parliament-approves-automated-monitoring-of-public-spaces-for-suspicious-behaviour/

53 J. Hendel, "Why suspected Chinese spy gear remains in America's telecom networks", Politico, July 21, 2022, https://www.politico.com/news/2022/07/21/us-telecom-companies-huawei-00047045

54 E. Morozov, "The Huawei war", Le Monde diplomatique, November 2020, https://mondediplo.com/2020/11/10huawei

55 Huawei, "Huawei launches Ascend 910, the world's most powerful AI processor, and MindSpore, an all-scenario AI computing framework", August 23, 2019, https://www.huawei.com/en/news/2019/8/huawei-ascend-910-most-powerful-ai-processor

56 Huawei, "Atlas 900 PoD (Model: 9000)", https://e.huawei.com/en/products/computing/ascend/atlas-900-pod-9000

57 Huawei, "Atlas 900 AI Cluster", https://e.huawei.com/en/products/computing/ascend/atlas-900-ai

58 Datagen, "ResNet-50: The Basics and a Quick Tutorial", https://datagen.tech/guides/computer-vision/resnet-50/

59 J. E. Hillman, M. McCalpin, "Watching Huawei's 'Safe Cities'", Center for Strategic and International Studies, November 4, 2019, https://www.csis.org/analysis/watching-huaweis-safe-cities

60 C. Zhihui, "Nowhere to hide: Building safe cities with technology enablers and AI", Huawei, July 2016, https://www.huawei.com/en/huaweitech/publication/winwin/ai/nowhere-to-hide

61 The content of the case study page was saved by an online archiving service and can be accessed here: https://archive.li/pZ9HO

62 SHARE Foundation, "Huawei knows everything about cameras in Belgrade – and they are glad to share!", March 29, 2019, https://www.sharefoundation.info/en/huawei-knows-everything-about-cameras-in-belgrade-and-they-are-glad-to-share/

63 Huawei, "Huawei Safe City Solution: Safeguards Serbia", August 23, 2018, accessible at: https://archive.li/pZ9HO

64 NEC, "NEC Face Recognition Technology Ranks First in NIST Accuracy Testing", October 3, 2019, https://www.nec.com/en/press/201910/global_20191003_01.html; NEC, "NEC Face Recognition Technology Ranks First in NIST Accuracy Testing", August 23, 2021, https://www.nec.com/en/press/202108/global_20210823_01.html

65 NEC, "NEC Unveils 'NEC Group AI and Human Rights Principles'", April 2, 2019, https://www.nec.com/en/press/201904/global_20190402_01.html

66 NEC, "NEC Group AI and Human Rights Principles", April 2, 2019, https://www.nec.com/en/press/201904/images/0201-01-01.pdf

67 F. Ragazzi et al., "Biometric and Behavioural Mass Surveillance in EU Member States", The Greens/EFA in the European Parliament, October 1, 2021, https://www.greens-efa.eu/biometricsurveillance/

68 R. Mahmud, "Brunei receives facial recognition equipment", Borneo Bulletin, March 15, 2022, https://borneobulletin.com.bn/brunei-receives-facial-recognition-equipment-2/

69 NEC, "NeoFace Watch", https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html

70 Ibid.

71 NEC Corporation of America, "The most accurate and fastest face recognition platform available:

NeoFace Watch", 2017, https://www.necam.com/docs/?id=3d1b0643-1d6e-4a9a-8195-a9ba79fe4b14

72 I. Burrington, "Why Amazon's Data Centers Are Hidden in Spy Country", The Atlantic, January 8, 2016, https://www.theatlantic.com/technology/archive/2016/01/amazon-web-services-data-center/423147/

73 Amazon, "Global Infrastructure", https://aws.amazon.com/about-aws/global-infrastructure/?pg=WIAWS

74 D. Harwell, "Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?", The Washington Post, April 30, 2019, https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/

75 Amazon, "We are implementing a one-year moratorium on police use of Rekognition", June 10, 2020, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition

76 J. Dastin, "Amazon extends moratorium on police use of facial recognition software", Reuters, May 18, 2021, https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

77 Amazon, "What is Amazon Rekognition?", https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html

78 IBM, "What is an API (application programming interface)?", https://www.ibm.com/topics/api

79 Amazon, "How Amazon Rekognition works", https://docs.aws.amazon.com/rekognition/latest/dg/how-it-works.html

80 R. Sauer, "Six principles to guide Microsoft's facial recognition work", Microsoft, December 17, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/

81 Microsoft, "What is Azure", https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

82 Microsoft, "What is the Azure Face service?", July 18, 2023, https://learn.mi-

crosoft.com/en-us/azure/cognitive-services/computer-vision/overview-identity

83 Ibid.

84 N. Crampton, "Microsoft's framework for building AI systems responsibly", Microsoft, June 21, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/21/microsofts-framework-for-building-ai-systems-responsibly/

85 S. Bird, "Responsible AI investments and safeguards for facial recognition", Microsoft, June 21, 2022, https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition/

86 Microsoft, "Use cases for Azure Face service", September 29, 2022, https://learn.microsoft.com/en-us/legal/cognitive-services/face/transparency-note

87 Autoriteit Persoonsgegevens, "AP: Pas op met camera's met gezichtsherkenning", October 29, 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-pas-op-met-camera%E2%80%99s-met-gezichtsherkenning (in Dutch)

88 Microsoft, "Use cases for Azure Face service", September 29, 2022, https://learn.microsoft.com/en-us/legal/cognitive-services/face/transparency-note

89 Ibid.

90 E. Jakubowska, "Do no harm? How the case of Afghanistan sheds light on the dark practice of biometric intervention", Heinrich Böll Stiftung EU, October 19, 2021, https://eu.boell.org/en/2021/10/19/do-no-harm-how-case-afghanistan-sheds-light-dark-practice-biometric-intervention

91 European Data Protection Board, European Data Protection Supervisor, "EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", June 18, 2021, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

92 Thales Group, "About Thales", https://www.thalesgroup.com/en/global/group

93 Thales Group, "Biometric Solutions", https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics

94 Thales Group, "Designing an ethical, socially accountable facial recognition system: A vision from Thales", 2021, https://www.thalesgroup.com/sites/default/files/database/document/2021-11/gov-wp-facial-recognition-2021.pdf, p. 10

95 Thales Group, "Video-based facial recognition - Thales Facial Recognition Platform", https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-software/live-face-identification-system

96 European Digital Rights (EDRi), "European Parliament: Make sure the AI act protects peoples' rights!", April 19, 2023, https://edri.org/wp-content/uploads/2023/04/PDF-FINAL-Statement-European-Parliament-Make-sure-the-AI-act-protects-peoples-rights.pdf

97 Thales Group, "Video-based facial recognition - Thales Facial Recognition Platform", https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-software/live-face-identification-system

98 European Digital Rights (EDRi), "IBM's facial recognition: the solution cannot be left to companies", July 17, 2020, https://edri.org/our-work/ibm-facial-recognition-solution-cannot-be-left-to-companies/

99 See, for example, analysis by French NGO La Quadrature du Net (LQDN) explaining why such data should be considered biometric data: La Quadrature du Net, "Loi J.O. : Refusons La Surveillance Biométrique", https://www.laquadrature.net/biometrie-jo/ (in French)

100 IPVM, "Huawei / Megvii Uyghur Alarms", December 8, 2020, https://ipvm.com/reports/huawei-megvii-uygur

101 BBC, "Who are the Uyghurs and why is China being accused of genocide?", May 21, 2022, https://www.bbc.co.uk/news/world-asia-china-22278037

102 IPVM, "Huawei / Megvii Uyghur Alarms", December 8, 2020, https://ipvm.com/reports/huawei-megvii-uygur

103 Ibid.

104 Amazon, "What is Amazon Rekognition?", https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html

105 Amazon, "Guidelines on face attributes", https://docs.aws.amazon.com/rekognition/latest/dg/guidance-face-attributes.html

106 M. Wood, "Thoughts On Machine Learning Accuracy", AWS News Blog, July 27, 2018, https://aws.amazon.com/blogs/aws/thoughts-on-machine-learning-accuracy/

107 Amazon, "FaceDetail - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_FaceDetail.html

108 Amazon, "Emotion - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_Emotion.html

109 Microsoft, "Use cases for Azure Face service", September 29, 2022, https://learn.microsoft.com/en-us/legal/cognitive-services/face/transparency-note

110 Microsoft, "Face detection and attributes", December 29, 2022, https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/concept-face-detection

111 S. Bird, "Responsible AI investments and safeguards for facial recognition", Microsoft, June 21, 2022, https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition

112 Microsoft, "Face detection and attributes", December 29, 2022, https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/concept-face-detection

113 Amazon, "Gender - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_Gender.html

114 Amazon, "KnownGender - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_KnownGender.html

115 Microsoft, "Face detection and attributes", July 26, 2023, https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/concept-face-detection

116 Amazon, "Landmark - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/APIReference/API_Landmark.html

117 Huawei, "Huawei Intelligent Video Surveillance Product Brochure", March 8, 2019, https://e.huawei.com/en/material/local/8cc4272f73664757977a5fd128e53a6c

118 Ibid.

119 Ibid.

120 Huawei, "NVR800 User Guide - Features", October 31, 2020, https://support.huawei.com/hedex/hdx.do?docid=EDOC1100166735&id=EN-US_TOPIC_0222303676, p. 10

121 Huawei, "NVR800 Distribution Solution 3.0 - Residential District", January 20, 2022, https://support.huawei.com/enterprise/en/doc/EDOC1100206847/691710f4/residential-district

122 Amazon, "People pathing - Amazon Rekognition", https://docs.aws.amazon.com/rekognition/latest/dg/persons.html

123 NEC Corporation of America, "The most accurate and fastest face recognition platform available: NeoFace Watch", 2017, https://www.necam.com/docs/?id=3d1b0643-1d6e-4a9a-8195-a9ba79fe4b14

124 Ibid.

125 A. Hern, "TechScape: Clearview AI was fined £7.5m for brazenly harvesting your data – does it care?", The Guardian, May 25, 2022, https://www.theguardian.com/technology/2022/may/25/techscape-clearview-ai-facial-recognition-fine

126 CNIL, "Facial recognition: 20 million euros penalty against Clearview AI", October 20, 2022, https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

127 European Data Protection Board, "Facial recognition: Italian SA fines Clearview AI EUR 20 million", March 10, 2022, https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

128 CNIL, "Facial recognition: the CNIL imposes a penalty payment on Clearview AI", May 10, 2023, available at: https://web.archive.org/web/20230614161044/https://www.cnil.fr/en/facial-recognition-cnil-imposes-penalty-payment-clearview-ai

129 Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta", February 2, 2021, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

130 ACLU of Illinois, "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law", May 9, 2022, https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

131 J. Clayton, B. Derico, "Clearview AI used nearly 1m times by US police, it tells

the BBC", BBC News, March 27, 2023, https://www.bbc.com/news/technology-65057011

132 Clearview AI, "Company Overview", https://www.clearview.ai/overview

133 R. Mac, C. Haskins, A. Pequeño IV, "Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here.", BuzzFeed News, August 25, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

134 European Data Protection Board, "Swedish DPA: Police unlawfully used facial recognition app", February 12, 2021, https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en

135 NOYB, "Complaint under Article 77(1), 80(1) GDPR, noyb Case-No: C043", May 26, 2021, https://noyb.eu/sites/default/files/2021-05/Clearview%20AI%20-%20EN%20DE%20-%20noyb%20-%20redacted.pdf, pp. 3-5

136 PimEyes, "PimEyes: Face Search Engine Reverse Image Search", https://pimeyes.com/en

137 Big Brother Watch, "Big Brother Watch files legal complaint against facial recognition 'search engine', Pimeyes", November 8, 2022, https://bigbrotherwatch.org.uk/2022/11/pimeyes-press-release/

138 PimEyes, "PimEyes' Statement on allegations made by Big Brother Watch", https://pimeyes.com/en/blog/pimeyes-statement-on-allegations-made-by-big-brother-watch

139 PimEyes, "More about PimEyes' database and opt-out service", https://pimeyes.com/en/blog/more-about-pimeyes-database-and-opt-out-service

140 European Parliament, "AI Act: a step closer to the first rules on Artificial Intelligence", May 11, 2023, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

141 "Enhanced face recognition in video - US9355301B2", Google Patents, https://patents.google.com/patent/US9355301B2/

142 Ibid.

143 "Sharing video footage from audio/video recording and communication devices for parcel theft deterrence - US10210727B2", Google Patents, https://patents.google.com/patent/US10210727B2/

144 Ibid.

145 "Grouping and ranking images based on facial recognition data - US9773156B2", Google Patents, https://patents.google.com/patent/US9773156B2/

146 Ibid.

147 "Face recognition in video content - US8494231B2", Google Patents, https://patents.google.com/patent/US8494231B2/

148 "Verifying identity based on facial dynamics - US10282530B2", Google Patents, https://patents.google.com/patent/US10282530B2/

149 "Adaptive image cropping for face recognition - US10872258B2", Google Patents, https://patents.google.com/patent/US10872258B2/

150 Clearview AI, "Clearview AI's Revolutionary Facial Recognition Platform Awarded U.S. Patent", January 31, 2022, https://www.clearview.ai/press-release-clearview-ais-revolutionary-facial-recognition-platform-awarded-us-patent

151 "Methods for Providing Information about a Person Based on Facial Recognition - US20210042527A1", Google Patents, https://patents.google.com/patent/US20210042527A1/

152 Ibid.

153 Ibid.

154 Ibid.

155 Ibid.

156 L. Rhue, "Racial Influence on Automated Perceptions of Emotions", November 9, 2018, https://dx.doi.org/10.2139/ssrn.3281765

157 Clearview AI, "Clearview AI Awarded U.S. Patent for Highly Accurate, Bias-Free Facial Recognition Algorithm", September 28, 2022, https://www.clearview.ai/clearview-ai-awarded-us-patent-for-highly-accurate-bias-free-facial-recognition-algorithm

158 "Scalable training data preparation pipeline and efficient distributed trainer for deep neural networks in facial recognition - US11443553B1", Google Patents, https://patents.google.com/patent/US11443553B1/

159 Ibid.

160 Y. Gorokhovskaia, A. Shahbaz, A. Slipowitz, "Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy", Freedom House, 2023, https://freedomhouse.org/report/freedom-world/2023/marking-50-years

161 A. Shahbaz, A. Funk, K. Vesteinsson, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet", Freedom House, 2022, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

162 E. Jakubowska, H. Maryam, M. Mahmoudi, "Retrospective facial recognition surveillance conceals human rights abuses in plain sight", Euronews, April 14, 2023, https://www.euronews.com/2023/04/14/retrospective-facial-recognition-surveillance-conceals-human-rights-abuses-in-plain-sight

163 J. Mudditt, "The nation where your 'faceprint' is already being tracked", BBC, June 24, 2022, https://www.bbc.com/future/article/20220616-the-nation-where-your-faceprint-is-already-being-tracked; J. Blakkarly, "Push for new law to regulate facial recognition technology", CHOICE, September 27, 2022, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/new-law-to-regulate-facial-recognition; M. Andrejevic et al., "How should we regulate the use of facial recognition in Australia?", Monash University, June 21, 2022, https://lens.monash.edu/@politics-society/2022/06/21/1384816/how-should-we-regulate-the-use-of-facial-recognition-in-australia

164 R. Crozier, "Govts agree on national face matching database", iTnews, October

5, 2017, https://www.itnews.com.au/news/govts-agree-on-national-face-matching-database-474759; C. Petrie, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019", Bills Digest No. 21, 2019–20, Parliament of Australia, August 26, 2019, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021#_Toc16773923

165 Australia's Federal Relations Architecture, "Intergovernmental Agreement on Identity Matching Services", October 5, 2017, https://federation.gov.au/about/agreements/intergovernmental-agreement-identity-matching-services Part 8

166 J. Hendry, "First states upload data to national facial recognition system", iTnews, September 17, 2019, https://www.itnews.com.au/news/first-states-upload-data-to-national-facial-recognition-system-531084; L. Pascu, "Western Australia joins national facial biometrics matching database", Biometric Update, April 2, 2020, https://www.biometricupdate.com/202004/western-australia-joins-national-facial-biometrics-matching-database; C. Petrie, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019", Bills Digest No. 21, 2019–20, Parliament of Australia, August 26, 2019, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021#_ftnref74

167 A. Macdonald, "Pending bill delays biometric data upload to drivers' license database in Australia", Biometric Update, October 13, 2020, https://www.biometricupdate.com/202010/pending-bill-delays-biometric-data-upload-to-drivers-license-database-in-australia; C. Tonkin, "Government building national facial recognition database", Australian Computer Society, February 1, 2022, https://ia.acs.org.au/article/2022/government-building-national-facial-recognition-database.html

168 S. Martin, "Committee led by Coalition rejects facial recognition database in surprise move", The Guardian, October 24, 2019, https://www.theguardian.com/australia-news/2019/oct/24/committee-led-by-coalition-rejects-facial-recognition-database-in-surprise-move

169 C. Petrie, "Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019", Bills Digest No. 21, 2019–20, Parliament of Australia, August 26, 2019, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd021#_Toc16773923

170 Report of the PJCIS is available here: Parliamentary Joint Committee on Intelligence and Security, "Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019", Parliament of Australia, 2019, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/AdvisoryreportontheIdentity-matchingServicesBill2019andtheAustralianPassportsAmendment(Identity-matchingServices)Bill2019.pdf;fileType=application%2Fpdf

171 J. Brookes, "Govt mulls facial recognition bill reheat", InnovationAus.com, January 16, 2023, https://www.innovationaus.com/govt-mulls-facial-recognition-bill-reheat/

172 Office of the Australian Information Commissioner, "Variation to extend term of MOU in relation to National Facial Biometric Matching Capability 2020", June 30, 2020, https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/national-facial-biometric-matching-capability/

variation-to-extend-term-of-mou-in-relation-to-national-facial-biometric-matching-capability-2020

173 J. Taylor, "Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards", The Guardian, June 30, 2021, https://www.theguardian.com/australia-news/2021/jul/01/calls-to-stop-nsw-police-trial-of-national-facial-recognition-system-over-lack-of-legal-safeguards

174 J. Taylor, "Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards", The Guardian, June 30, 2021, https://www.theguardian.com/australia-news/2021/jul/01/calls-to-stop-nsw-police-trial-of-national-facial-recognition-system-over-lack-of-legal-safeguards; J. Hendry, "Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards", InnovationAus.com, October 11, 2022, https://www.innovationaus.com/facial-recognition-use-misunderstood-nsw-police/

175 E. Tlozek, "SA Police could use Adelaide city facial recognition technology, despite being asked not to", ABC News, June 19, 2022, https://www.abc.net.au/news/2022-06-20/sa-police-could-use-adelaide-city-facial-recognition-technology/101166064

176 C. Kelly, "Protesters 'should expect' Australian police to use facial recognition", The New Daily, June 13, 2020, https://thenewdaily.com.au/news/2020/06/13/facial-recognition-police-protest/; J. Brookes, "Facial recognition and the NSW protest crowds", InnovationAus.com, July 27, 2021, https://www.innovationaus.com/facial-recognition-and-the-nsw-protest-crowds/

177 B. Kaye, "Australia's two largest states trial facial recognition software to police pandemic rules", Reuters, September 17, 2021, https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/

178 S. Grill, "CHOICE raises concern over Bunnings, Kmart and the Good Guys use of facial recognition technology", ABC News, June 15, 2022, https://www.abc.net.au/news/2022-06-15/choice-investigation-major-retailers-using-facial-recognition/101153384

179 J. Taylor, "7-Eleven took photos of some Australian customers' faces without consent, privacy commissioner rules", The Guardian, October 14, 2021, https://www.theguardian.com/australia-news/2021/oct/14/7-eleven-took-photos-of-some-australian-customers-faces-without-consent-privacy-commissioner-rules

180 Office of the Australian Information Commissioner, "OAIC and UK's ICO open joint investigation into Clearview AI Inc.", July 9, 2020, https://www.oaic.gov.au/newsroom/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc

181 Australian Human Rights Commission, "Facial recognition & biometric tech", https://tech.humanrights.gov.au/artificial-intelligence/facial-recognition-biometric-tech; Australian Human Rights Commission, "Australians deserve tech that protects their rights", May 27, 2021, https://humanrights.gov.au/about/news/media-releases/australians-deserve-tech-protects-their-rights

182 N. Davis, L. Perry, E. Santow, "Facial recognition technology: Towards a model law", Human Technology Institute, The University of Technology Sydney, September 2022, https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf

183 The Parliamentary Joint Committee on Human Rights (PJCHR) is estab-

lished by the Human Rights (Parliamentary Scrutiny) Act 2011: Parliament of Australia, Human Rights (Parliamentary Scrutiny) Act 2011, No. 186, https://www.legislation.gov.au/Details/C2016C00195; The committee's main function is to examine all bills and legislative instruments for compatibility with human rights, as these rights are defined in the act itself, see: Australian Human Rights Commission, "Parliamentary Joint Committee on Human Rights",https://humanrights.gov.au/our-work/rights-and-freedoms/parliamentary-joint-committee-human-rights

184 Full article: A. Fletcher, "Government surveillance and facial recognition in Australia: a human rights analysis of recent developments", Griffith Law Review, 32:1, 30-61, 2023, https://doi.org/10.1080/10383441.2023.2170616

185 History of most important amendments is available here: Office of the Australian Information Commissioner, "History of the Privacy Act", https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/history-of-the-privacy-act

186 The latest version is available here: Parliament of Australia, Privacy Act 1988, No. 119, https://www.legislation.gov.au/Details/C2022C00361

187 Office of the Australian Information Commissioner, "Biometric scanning",https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning

188 This aspect of the biometric information regulation in the Privacy Act has been criticised as inadequate and outdated, see: S. Burns et al., "Facial recognition and artificial intelligence in Australia. Do we need more rules?", Gilbert + Tobin, July 25, 2022,https://www.gtlaw.com.au/knowledge/facial-recognition-artificial-intelligence-australia-do-we-need-more-rules

189 According to the OAIC interpretation, the four key elements of consent are: the individual is adequately informed before giving consent, the individual gives consent voluntarily, the consent is current and specific, and the individual has the capacity to understand and communicate their consent,see: Office of the Australian Information Commissioner, "Australian Privacy Principles guidelines", Chapter B, December 21, 2022, https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#consent

190 Clause 3.4.(a) of the Principle 3 of Australian Privacy Principles guidelines.

191 Clause 3.4. (d) of the Principle 3 of Australian Privacy Principles guidelines.

192 N. Davis, L. Perry, E. Santow, "Facial recognition technology: Towards a model law", Human Technology Institute, The University of Technology Sydney, September 2022, https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf p. 37

193 Office of the Australian Information Commissioner, "OAIC and UK's ICO open joint investigation into Clearview AI Inc", July 9, 2020,https://www.oaic.gov.au/newsroom/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc.

194 Office of the Australian Information Commissioner, "OAIC and ICO conclude joint investigation into Clearview AI", November 3, 2021, https://www.oaic.gov.au/newsroom/oaic-and-ico-conclude-joint-investigation-into-clearview-ai

195 Whole text of the determination is available here: Australian Information Commissioner, "Commissioner initiated investigation into Clearview AI, Inc.

(Privacy) [2021] AICmr 54", October 14, 2021, http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html

196 Office of the Australian Information Commissioner, "Clearview AI breached Australians' privacy", November 3, 2021, https://www.oaic.gov.au/newsroom/clearview-ai-breached-australians-privacy

197 Ibid.

198 J. Siganto, "Clearview AI Australia Found To Have Breached Privacy Laws", Privacy 108, March 18, 2022, https://privacy108.com.au/insights/clearview-ai-australia-privacy-breach/

199 Whole text of the determination is available here: Australian Information Commissioner, "Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74", November 26, 2021, http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/74.html

200 Office of the Australian Information Commissioner, "AFP ordered to strengthen privacy governance", December 16, 2021, https://www.oaic.gov.au/newsroom/afp-ordered-to-strengthen-privacy-governance

201 R. Mac, C. Haskins, A. Pequeño IV, "Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here.", BuzzFeed News, August 25, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

202 Office of the Privacy Commissioner of Canada, "RCMP's use of Clearview AI's facial recognition technology violated Privacy Act, investigation concludes", June 10, 2021, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/

203 Office of the Privacy Commissioner of Canada, "Announcement: Clearview AI ordered to comply with recommendations to stop collecting, sharing images", December 14, 2021, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/

204 M. Forrest, "RCMP's use of facial recognition extends well beyond Clearview AI", Politico, September 30, 2022, https://www.politico.com/news/2022/09/30/rcmps-facial-recognition-clearview-ai-00059639

205 Office of the Privacy Commissioner of Canada, "Recommended legal framework for police agencies' use of facial recognition", May 2, 2022, https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/s-d_prov_20220502/

206 P. Kelly, "Facial Recognition Technology and the Growing Power of Artificial Intelligence", House of Commons of Canada Standing Committee on Access to Information, Privacy and Ethics, October 2022, https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf

207 Internet Policy & Public Interest Clinic (CIPPIC), "Facial Recognition at a Crossroads: Transformation at our Borders & Beyond ", September 2020, https://cippic.ca/uploads/FR_Transforming_Borders.pdf

208 International Civil Liberties Monitoring Group, "Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies", July 8, 2020, https://iclmg.ca/wp-content/uploads/2020/07/facial-recognition-letter-08072020.pdf

209 Department of Justice of Canada, The Canadian Charter of Rights and Freedoms, https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/

210 Parliament of Canada, Revised Statutes of Canada, Privacy Act (1985, c. P-21), last amended 2022, https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html

211 Parliament of Canada, Statutes of Canada, Personal Information Protection and Electronic Documents Act (2000, c. 5), last amended 2019, https://laws-lois.justice.gc.ca/eng/acts/p-8.6/

212 The Government of Canada, Directive on Automated Decision-Making, 2019, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

213 Parliament of Canada, C-27 (44-1), 2022, https://www.parl.ca/legisinfo/en/bill/44-1/c-27

214 Office of the Privacy Commissioner of Canada, "Summary of privacy laws in Canada", January 2018, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

215 P. Backman, C. Kennedy, "Biometric Identification and Privacy Concerns: A Canadian Perspective", Aird & Berlis LLP, https://www.airdberlis.com/docs/default-source/articles/biometric-identification-and-privacy-concerns.pdf?

216 Office of the Privacy Commissioner of Canada, "Announcement: OPC updates guidance regarding sensitive information", August 13, 2021, https://priv.gc.ca/en/opc-news/news-and-announcements/2021/an_210813/

217 Parliament of Canada, C-27 (44-1), Section 63, 2022, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

218 Innovation, Science and Economic Development Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion document", March 13, 2023, https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

219 National Assembly of Quebec, Act to establish a legal framework for information technology C-1.1, 2001, https://www.legisquebec.gouv.qc.ca/en/document/cs/c-1.1

220 P. Kelly, "Facial Recognition Technology and the Growing Power of Artificial Intelligence", House of Commons of Canada Standing Committee on Access to Information, Privacy and Ethics, October 2022, https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf, p. 58

221 Ibid., p. 54

222 Supreme Court of Canada, "R. v. Dyment", December 8, 1988, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do

223 Supreme Court of Canada, "R. v. Spencer", June 13, 2014, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

224 Federal Court of Appeal of Canada, "Wansink v. Telus Communications Inc.", January 1, 2007, https://decisions.fca-caf.gc.ca/fca-caf/decisions/en/item/35446/index.do

225 Canadian HR Reporter, "Employer can't use finger scan system to clock employees", January 29, 2007, https://www.hrreporter.com/focus-areas/employ-

ment-law/legal-briefs/287904

226 L. McGrady, M. Koroneos, "Employee Privacy Rights in the Workplace", Faculty of Law Center for Law in the Contemporary Workplace – Queen's University, November 22, 2013, https://clcw.queenslaw.ca/sites/clcwwww/files/files/Powerpoints%20Papers/Privacy/Leo%20McGrady%20Employee%20Privacy%20Rights%20in%20the%20Workplace.pdf

227 D. Gershgorn, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", OneZero, Mar 2, 2021, https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015

228 Ibid.

229 Y. Li, M. Elfstrom, "Does Greater Coercive Capacity Increase Overt Repression? Evidence from China", Journal of Contemporary China, 2021, 30:128, 186-211, https://doi.org/10.1080/10670564.2020.1790898

230 A. Polyakova, C. Meserole, "Exporting digital authoritarianism", Brookings, 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

231 Ibid.

232 AFP, "Sinister or safer? China takes the lead in using facial recognition technology", Hong Kong Free Press, October 21, 2017, https://hongkongfp.com/2017/10/21/sinister-safer-china-takes-lead-using-facial-recognition-technology/

233 J. Vincent, "Chinese police are using facial recognition sunglasses to track citizens", The Verge, February 8, 2018, https://www.theverge.com/2018/2/8/16990030/china-facial-recognition-sunglasses-surveillance

234 AFP, "Sinister or safer? China takes the lead in using facial recognition technology", Hong Kong Free Press, October 21, 2017, https://hongkongfp.com/2017/10/21/sinister-safer-china-takes-lead-using-facial-recognition-technology/

235 D. Gershgorn, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", Center for Security and Emerging Technology, March 2, 2021, https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/

236 D. Byler, "Because There Were Cameras, I Didn't Ask Any Questions", ChinaFile, December 30, 2020, https://www.chinafile.com/extensive-surveillance-china; IPVM, "Huawei / Megvii Uyghur Alarms", December 8, 2020, https://ipvm.com/reports/huawei-megvii-uygur

237 A. Polyakova, C. Meserole, "Exporting digital authoritarianism", Brookings, 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

238 Ibid.

239 Ibid.

240 D. Byler, "Because There Were Cameras, I Didn't Ask Any Questions", ChinaFile, December 30, 2020, https://www.chinafile.com/extensive-surveillance-china

241 J. Tang, "China casts its 'SkyNet' far and wide, pursuing tens of thousands who

flee overseas", Radio Free Asia, May 4, 2022, https://www.rfa.org/english/news/china/skynet-repatriation-05042022151054.html

242 A. Polyakova, C. Meserole, "Exporting digital authoritarianism", Brookings, 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf

243 M. Carney, "Leave no dark corner", ABC News, September 17, 2018, https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278; P. Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras", The New York Times, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html;

244 J. Chin, L. Lin, "Surveillance state : inside China's quest to launch a new era of social control", St. Martin's Press, 2022, https://archive.org/details/surveillancestat0000chin; R. Andersen, "The Panopticon Is Already Here", The Atlantic, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/; D. Tang, "Chinese AI 'can check loyalty of party members'", The Sunday Times, July 4, 2022, https://www.thetimes.co.uk/article/chinese-ai-can-check-loyalty-of-party-members-92d97hgwv; S. Chestnut Greitens, "Dealing With Demand For China's Global Surveillance Exports", Brookings, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf

245 J. E. Hillman, M. McCalpin, "Watching Huawei's 'Safe Cities'", Center for Strategic & International Studies, November 4, 2019, https://www.csis.org/analysis/watching-huaweis-safe-cities

246 R. Standish, "The Fight In Serbia Over Chinese-Style Surveillance (Part 1)", Radio Free Europe/ Radio Liberty, November 22, 2022, https://www.rferl.org/a/serbia-chinese-surveilllance-backlash-standish/32142771.html

247 Human Rights in China, "Regulatory framework, Surveillance industry in China", February 15, 2019, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/HUMAN_RIGHTS_IN_CHINA.pdf;

248 Ibid.

249 Ibid.

250 European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

251 International Association of Lawyers, "A Constitutional View of Privacy Rights in China", October 19, 2020, https://www.uianet.org/en/news/constitutional-view-privacy-rights-china

252 An English translation of the law is available here: National People's Congress, Civil Code of the People's Republic of China, 2020, http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf

253 D. Luo, Y. Wang, "China - Data Protection Overview", DataGuidance, November 2022, https://www.dataguidance.com/notes/china-data-protection-over-

view

254 English translation of the law is available here: National People's Congress, Personal Information Protection Law of the People's Republic of China, 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

255 English translation of the law is available here: DataGuidance, Cybersecurity Law 2016 (Unofficial translation), 2016, https://www.dataguidance.com/legal-research/cybersecurity-law-2016-unofficial-translation

256 English translation of the law is available here: National People's Congress, Data Security Law of the People's Republic of China, 2021, http://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.htm

257 English translation of the law is available here: National People's Congress, National Security Law, 2015, https://www.chinalawtranslate.com/en/2015nsl/

258 English translation of the law is available here: National People's Congress, Counter-Terrorism Law (as amended in 2018), 2015, https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/

259 English translation of the law is available here: National People's Congress, PRC National Intelligence Law (as amended in 2018), 2017, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

260 Human Rights in China, "Regulatory framework, Surveillance industry in China", February 15, 2019, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Surveillance/HUMAN_RIGHTS_IN_CHINA.pdf

261 AnJie Broad Law Firm, "The Privacy, Data Protection and Cybersecurity Law Review: China", The Law Review, October 27, 2022, https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china

262 Summary provided on the website of the Supreme People's Court is available here: Supreme People's Court of the People's Republic of China, "New rules to curb misuse of facial recognition tech", July 29, 2021, https://perma.cc/3YPC-CPV4

263 Ibid.

264 Text in English is available here: National Standard of the People's Republic of China, "Information security technology–Personal information (PI) security specification", 2020, https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf

265 Text of the draft in English is available here: National Technical Committee for the Standardization of Information Security of China, "Information Security Technology Security - Requirements for Facial Recognition Data", 2021, https://www.chinalawtranslate.com/en/draft-facial-recognition-standards/

266 Article 2 of the Cybersecurity Law.

267 S. Xuanfeng Ning, H. Wu, "Data Protection Laws and Regulations China 2022-2023", The International Comparative Legal Guides, 2022, https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

268 AnJie Broad Law Firm, "The Privacy, Data Protection and Cybersecurity Law Review: China", The Law Review, October 27, 2022, https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china

269 Ibid.

270 Y. Luo, R. Guo, "Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead" , 25 U. Pa. J.L. & Soc. Change 153, 2021, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1269&context=jlasc, p. 164

271 Timeline of adoption available here: Digital Policy Alert, "China: Information Security Technology Face Recognition Data Security Requirements", https://digitalpolicyalert.org/change/1859-information-security-technology-face-recognition-data-security-requirements

272 Garrigues, "China's Supreme People's Court sets rules for facial recognition technology", August 2, 2021, https://www.garrigues.com/en_GB/new/chinas-supreme-peoples-court-sets-rules-facial-recognition-technology

273 X. Shen, "China's first facial-recognition lawsuit comes to an end with new ruling and new questions about the fate of individuals' data", South China Morning Post, April 12, 2021, https://www.scmp.com/tech/policy/article/3129226/chinas-first-facial-recognition-lawsuit-comes-end-new-ruling-and-new?module=perpetual_scroll_0&pgtype=article&campaign=3129226

274 G. Du, L. Qiang , "China's First Facial Recognition Case", China Justice Observer, May 2, 2021, https://www.chinajusticeobserver.com/a/china-s-first-facial-recognition-case

275 Y. Du, "China's First Face Recognition Case Study", HG.org Legal Resources, https://www.hg.org/legal-articles/china-s-first-face-recognition-case-study-58943

276 Y. Ye, "Hangzhou Court Rules in Landmark Facial Recognition Case", Sixth Tone, November 21, 2020, https://www.sixthtone.com/news/1006479

277 G. Du, L. Qiang , "China's First Facial Recognition Case", China Justice Observer, May 2, 2021, https://www.chinajusticeobserver.com/a/china-s-first-facial-recognition-case

278 Y. Du, "China's First Face Recognition Case Study", HG.org Legal Resources, https://www.hg.org/legal-articles/china-s-first-face-recognition-case-study-58943

279 AnJie Broad Law Firm, "The Privacy, Data Protection and Cybersecurity Law Review: China", The Law Review, October 27, 2022, https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china

280 X. Ying , Y. Suwen, "About Face", NewsChina Magazine, http://www.newschinamag.com/newschina/articleDetail.do?article_id=7219&section_id=17&magazine_id=81

281 Dentons, "China's highest court clarifies judicial rules in civil disputes related to face recognition technology", August 2, 2021, https://www.dentons.com/en/insights/articles/2021/august/2/china-highest-court-clarifies-judicial-rules-in-civil-disputes

282 CIPESA, "State of Internet Freedom in Africa 2022: The Rise of Biometric Surveillance", September 29, 2022, https://cipesa.org/2022/09/state-of-internet-freedom-in-africa-2022-the-rise-of-biometric-surveillance/; H. Swart, A. Munoriyarwa, "Video Surveillance in Southern Africa: Case studies of security camera systems in the region", Media Policy and Democracy Project, May 2020,https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_re-

gion.pdf

283 Some reports on this influence from a US perspective can be found here: United States-China Economic and Security Review Commission, "Hearing On China's Strategic Aims In Africa", 2020,https://www.uscc.gov/sites/default/files/2020-06/May_8_2020_Hearing_Transcript.pdf or in EPIC series available here: B. Jili, "The Rise of Chinese Surveillance Technology in Africa (part 1 of 6)", EPIC, May 31, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (part 2 of 6)", EPIC, June 29, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-2/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (part 3 of 6)", EPIC, July 29, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-3-of-6/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (part 4 of 6)", EPIC, August 25, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-4-of-6/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (part 5 of 6)", EPIC, September 22, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-5-of-6/; B. Jili, "The Rise of Chinese Surveillance Technology in Africa (part 6 of 6)", EPIC, October 21, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-6-of-6/

284 Baker McKenzie, "How the European Union's General Data Protection Regulations influenced data privacy law in Africa", June 1, 2022, https://www.bakermckenzie.com/en/newsroom/2022/05/eu-general-data-protection-regulations; P. Boshe, M. Hennemann, "Rule of Law Programme Middle East and North Africa - Data Protection Laws in Northern Africa - Regulatory Approaches, Key Principles, Selected Instruments", Konrad-Adenauer-Stiftung, September 2022, https://www.kas.de/en/web/rspno/single-title/-/content/data-protection-laws-in-northern-africa-regulatory-approaches-key-principles-selected-documents

285 Artificial intelligence (AI) system designed to identify individuals from a distance by comparing their biometric data with the data stored in a reference database or data repository.

286 F. Ragazzi et al., "Biometric and Behavioural Mass Surveillance in EU Member States", The Greens/EFA in the European Parliament, October 1, 2021, https://www.greens-efa.eu/biometricsurveillance/

287 E. De Marco, Aeris, "Impacts of the use of biometric and behavioural mass surveillance technologies on human rights and the rule of law", The Greens/EFA in the European Parliament, February 2022, https://extranet.greens-efa-service.eu/public/media/file/1/7487

288 VIS - Visa Information System, SIS - Schengen Information System, ECRIS - European Criminal Records System, ETIAS - European Travel Information and Authorisation System, EES - Entry/Exit System.

289 European Union's Fundamental Rights Agency, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

290 European Digital Rights (EDRi), "New EU law amplifies risks of state over-reach and mass surveillance", September 7, 2022, https://edri.org/our-work/new-eu-law-amplifies-risks-of-state-over-reach-and-mass-surveillance/

291 P. De Hert, G. Bouchagiar, "Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices?", Information Polity 27, 193-217, 2022, https://orbilu.uni.lu/bitstream/10993/51103/2/ip_2022_27-2_ip-27-2-ip211525_ip-27-ip211525.pdf

292 L. Edwards, "Expert explainer: The EU AI Act proposal", Ada Lovelace Institute, April 8, 2022, https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/

293 M. Heikkila, "European Parliament calls for a ban on facial recognition", Politico, October 6, 2021 https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/

294 C. Thorbecke, "Citing human rights risks, UN calls for ban on certain AI tech until safeguards are set up", ABC News, September 15, 2021, https://abcnews.go.com/Technology/citing-human-rights-risks-calls-ban-ai-tech/story?id=80034073

295 L. Peets et al., "European Parliament Votes in Favor of Banning the Use of Facial Recognition in Law Enforcement", Covington Inside Privacy, October 12, 2021, https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/

296 European Data Protection Board, "EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", June 21, 2021, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

297 Amnesty International, "Amnesty International and more than 170 organisations call for a ban on biometric surveillance", June 7, 2021, https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/

298 Reclaim Your Face, https://reclaimyourface.eu/

299 E. Pollina, F. Maccioni, "Italy outlaws facial recognition tech, except to fight crime", Reuters, November 14, 2022, https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/

300 M. Heikkila, "German coalition backs ban on facial recognition in public places", Politico, November 24, 2021, https://www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/

301 Reclaim Your Face, "Portugal: Proposed law tries to sneak in biometric mass surveillance", November 15, 2021, https://reclaimyourface.eu/portugal-proposed-law-tries-to-sneak-in-biometric-mass-surveillance/

302 A. Lodie, S. Celis Juarez, "AI-Assisted Security at the Paris 2024 Olympic Games: From Facial Recognition to Smart Video", AI Regulation, January 27, 2023, https://ai-regulation.com/ai-driven-systems-paris-olympics/

303 MEP Patrick Breyer, "Expect biometric mass surveillance in Paris in 2024: French Parliament approves automated monitoring of public spaces for 'suspicious behaviour'", Patrick-Breyer.de, March 24, 2023, https://www.patrick-breyer.de/en/expect-biometric-mass-surveillance-in-paris-in-2024-french-parliament-approves-automated-monitoring-of-pub-

lic-spaces-for-suspicious-behaviour/

304 MEP Patrick Breyer, "Vote to stop a future of biometric mass surveillance in Europe!", Patrick-Breyer.de, March 17, 2023, https://www.patrick-breyer.de/wp-content/uploads/2023/03/MEP-letter-to-FR-MPs-about-biometric-mass-surveillance-in-2024-Olympic-law.pdf

305 N. Aszódi, "Open letter: the German government should stand up for a strong ban on biometric surveillance in the Council of EU negotiations regarding the AI Act", AlgorithmWatch, November 8, 2022, https://algorithmwatch.org/en/open-letter-german-government-biometric-surveillance-ai-act/

306 European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

307 European Union, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

308 European Commision, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-%3A52021PC0206

309 GDPR, Article 4 (14); LED, Article 3 (13).

310 Article 29 Data Protection Working Party, "Opinion 3/2012 on developments in biometric technologies", April 27, 2012, https://www.pdpjournals.com/docs/87998.pdf

311 GDPR, Article 9, Paragraph 1; LED, Article 10.

312 S. Barros Vale, G. Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities", The Future of Privacy Forum, May 2022, https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf, p. 41

313 European Digital Rights (EDRi), "European Parliament calls loud and clear for a ban on biometric mass surveillance in AI Act", September 14, 2022, https://edri.org/our-work/european-parliament-calls-loud-and-clear-for-a-ban-on-biometric-mass-surveillance-in-ai-act/

314 European Data Protection Board, "EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination", June 21, 2021, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en

315 Council of the European Union, "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", December 6, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artifi-

cial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

316 European Parliament, "AI Act: a step closer to the first rules on Artificial Intelligence", May 11, 2023, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

317 European Parliament, "MEPs ready to negotiate first-ever rules for safe and transparent AI", June 14, 2023, https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

318 European Digital Rights (EDRi), "EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act", June 14, 2023, https://edri.org/our-work/eu-parliament-plenary-ban-of-public-facial-recognition-human-rights-gaps-ai-act/; Access Now, "Historic vote in the European Parliament: dangerous AI surveillance banned, but not for migrant people at the borders", June 14, 2023, https://www.accessnow.org/press-release/historic-vote-in-the-european-parliament-dangerous-ai-surveillance-banned-but-not-for-migrant-people-at-the-borders/

319 L. R. Helfer, E. Voeten, "International Courts as Agents of Legal Change: Evidence from LGBT Rights in Europe", 68 International Organization 77-110, 2014, https://scholarship.law.duke.edu/faculty_scholarship/2402/

320 M. Brkan, "The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core", European Constitutional Law Review, Volume 14, Issue 2, June 2018, pp. 332 - 368, https://doi.org/10.1017/S1574019618000159

321 European Court of Human Rights, "Case of S. and Marper v. the United Kingdom", December 4, 2008, https://rm.coe.int/168067d216

322 European Court of Human Rights, "Gaughran v. The United Kingdom", February 13, 2020, https://hudoc.echr.coe.int/en?i=002-12731

323 European Court of Human Rights, "Case of Uzun v. Germany", September 2, 2010, https://hudoc.echr.coe.int/en?i=001-100293

324 The Court of Justice of the European Union, "La Quadrature du Net and Others", October 6, 2020, https://curia.europa.eu/juris/liste.jsf?language=en&num=c-511/18&td=ALL

325 Article 19, "When bodies become data: Biometric technologies and freedom of expression", April 2021, https://www.article19.org/wp-content/uploads/2021/05/Biometric-Report-P3-min.pdf

326 European Data Protection Board, "Facial recognition in school renders Sweden's first GDPR fine", August 22, 2019, https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv

327 CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position", October 29, 2019, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dansdeux-lycees-la-cnil-precise-sa-position (in French); European Data Protection Board, "Fine for processing students' fingerprints imposed on a school", March 5, 2020, https://edpb.europa.eu/news/national news/2020/fine-processing-students-fingerprints-imposed-school_en; S. Weale, "ICO to step in after schools use facial

recognition to speed up lunch queue", The Guardian, October 18, 2021,https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to speed-up-lunch-queue-ayrshire-technology-payments-uk; Tribunal Administratif de Marseille, "Laquadrature du net et autres", February 27, 2020, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249. pdf (in French)

328 European Data Protection Board, "Swedish DPA: Police unlawfully used facial recognition app", February 12, 2021, https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en

329 Garante per la Protezione dei Dati Personali, "Facial recognition: the SARI Real Time system is not compliant with privacy laws", April 16, 2021, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575842

330 European Data Protection Board, "News", https://edpb.europa.eu/news/news_en

331 Based on this report: Common Cause, Lokniti – Centre for the Study Developing Societies (CSDS), "Status of Policing in India Report 2023: Surveillance and the Question of Privacy", 2023, https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf; Indian police have extensive plans for predictive policing, whereas FRT's role in its implementation remains to be seen.

332 Internet Freedom Foundation, Panoptic, "About", https://panoptic.in/about

333 The figure varies in different reports, from 440,000: P. Bischoff, "Surveillance Camera Statistics: Which City has the Most CCTV Cameras?", Comparitech, May 23, 2023, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; to 900,000: Q. Inzamam, H. Qadri, "This Part of India Is on the Verge of Becoming a Complete Surveillance State", Slate, July 13, 2022, https://slate.com/technology/2022/07/telangana-india-surveillance-state.html

334 Amnesty International, "Ban The Scan Hyderabad", https://banthescan.amnesty.org/hyderabad/#num-14

335 R. R. Jain, "Facial recognition wielded in India to enforce COVID policy", AP News, December 20, 2022, https://apnews.com/article/technology-health-india-hyderabad-law-enforcement-9b5e249d7ef5cefd3c6dc74c2c4b5b84

336 India's national Crime and Criminal Tracking Networks and Systems (CCTNS), which is a nationwide database that contains millions of images of criminals and missing people: Q. Inzamam, H. Qadri, "This Part of India Is on the Verge of Becoming a Complete Surveillance State", Slate, July 13, 2022, https://slate.com/technology/2022/07/telangana-india-surveillance-state.html

337 Al Jazeera, "Facial recognition taken to court in India's surveillance hotspot", January 20, 2022, https://www.aljazeera.com/news/2022/1/20/india-surveillance-hotspot-telangana-facial-recognition-court-lawsuit-privacy; R. R. Jain, "Facial recognition wielded in India to enforce COVID policy", AP News, December 20, 2022, https://apnews.com/article/technology-health-india-hyderabad-law-enforcement-9b5e249d7ef5cefd3c6dc74c2c4b5b84

338 V. Bansal, "Meet the man who sued an Indian state over police facial recognition technology", The Record, February 10, 2022, https://therecord.media/meet-the-man-who-sued-an-indian-state-over-facial-recognition-technology; K. Bapat, "Telangana High Court issues notice in India's first legal challenge to

the deployment of Facial Recognition Technology", Internet Freedom Foundation, January 3, 2022, https://internetfreedom.in/telangana-high-court-issues-notice-in-indias-first-legal-challenge-to-the-deployment-of-facial-recognition-technology/

339 A. Ghosh, "Facial Recognition Is Out of Control in India", Vice, June 13, 2022, https://www.vice.com/en/article/akew98/facial-recognition-is-out-of-control-in-india

340 N.T. Sarasvati, "How facial recognition-based surveillance restricted this Hyderabad resident's freedoms", MediaNama, January 10, 2023, https://www.medianama.com/2023/01/223-facial-recognition-surveillance-tactics-hyderabad-resident-constitutional-freedoms/

341 H. Suresh, "Why Hyderabad became India's surveillance capital", The News Minute, December 7, 2021, https://www.thenewsminute.com/article/why-hyderabad-became-india-s-surveillance-capital-158466; K. Sambhav, "EXCLUSIVE: Telangana Offered Its Own 360 Degree Citizen Tracking System To Modi Govt", HuffPost, March 18, 2020, https://www.huffpost.com/archive/in/entry/telangana-samagram-system-social-registry_in_5e721e19c5b-63c3b64881b30; K. Sambhav, "EXCLUSIVE: Telangana Offered Its Own 360 Degree Citizen Tracking System To Modi Govt", The Reporters' Collective, March 19, 2020, https://www.reporters-collective.in/stories/exclusive-telangana-offered-its-own-360-degree-citizen-tracking-system-to-modi-govt

342 Al Jazeera, "India's Telangana to test facial recognition in local elections", January 22, 2020, https://www.aljazeera.com/news/2020/1/22/indias-telangana-to-test-facial-recognition-in-local-elections

343 The most surveilled Indian city, although five times less populated, is Indore, see: P. Bischoff, "Surveillance Camera Statistics: Which City has the Most CCTV Cameras?", Comparitech, May 23, 2023, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; M. Lu, "Ranked: The World's Most Surveilled Cities", Visual Capitalist, October 6, 2022, https://www.visualcapitalist.com/ranked-the-worlds-most-surveilled-cities/

344 S. Santoshini, "Indian police use facial recognition to persecute Muslims and other marginalized communities", Coda Story, October 11, 2022, https://www.codastory.com/authoritarian-tech/india-police-facial-recognition/; Hindustan Times, "2 yrs after Delhi riots: 2,456 held, 2 convicted", February 24, 2022, https://www.hindustantimes.com/cities/delhi-news/2-yrs-after-delhi-riots-2-456-held-2-convicted-101645660761884.html

345 A. Jain, "Delhi Police's claims that FRT is accurate with a 80% match are 100% scary", Internet Freedom Foundation, August 17, 2022, https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/

346 Hindustan Times, "India's use of facial recognition tech during protests causes stir", August 20, 2022, https://tech.hindustantimes.com/tech/news/india-s-use-of-facial-recognition-tech-during-protests-causes-stir-story-lL-6fRtv9K43vrwWhuowA2M.html

347 NDTV, "Facial Recognition For Entry To Indian Airports Begins", December 2, 2022, https://www.ndtv.com/india-news/at-3-airports-in-india-facial-recognition-based-entry-from-today-3568817; N. Deuskar, "Facial recognition system rollout at Indian airports raises privacy concerns", Scroll, December 14, 2022, https://scroll.in/article/1038975/facial-recognition-system-roll-out-at-indian-airports-raises-privacy-concerns

348 N. Deuskar, "Facial recognition system rollout at Indian airports raises privacy concerns", Scroll, December 14, 2022, https://scroll.in/article/1038975/facial-recognition-system-rollout-at-indian-airports-raises-privacy-concerns

349 A. Kimery, "India set to stand up world's largest government facial recognition database for police use", Biometric Update, March 11, 2020, https://www.biometricupdate.com/202003/india-set-to-stand-up-worlds-largest-government-facial-recognition-database-for-police-use

350 A. Jain, "NCRB's National Automated Facial Recognition System", June 7, 2023, https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system

351 N. Ohri, "India lets banks use face recognition, iris scan for some transactions - sources", Reuters, January 13, 2023, https://www.reuters.com/world/india/india-lets-banks-use-face-recognition-iris-scan-some-transactions-sources-2023-01-13/; R. Jain, "Indian government to add facial recognition, iris scan for digital payments", Business Insider India, February 17, 2020, https://www.businessinsider.in/tech/news/indian-government-to-add-facial-recognition-iris-scan-for-digital-payments/articleshow/74176902.cms

352 R. C. Bajpai, S. Yadav, "Use of Facial Recognition Technology in India: A Function Creep Breaching Privacy", Oxford Human Rights Hub, January 11, 2021, https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/

353 R. K. George, A. Tom, "Update on withdrawal of the personal data protection bill, 2019", Lexology, August 10, 2022, https://www.lexology.com/library/detail.aspx?g=0c082211-6ba5-402c-9623-32c5e4165d45; Times of India, "Centre withdraws Personal Data Protection Bill, 2019: Will present new legislation, says IT minister", August 3, 2022, https://timesofindia.indiatimes.com/india/centre-withdraws-personal-data-protection-bill/articleshow/93323625.cms

354 Draft of the bill is available here: Ministry of Electronics & Information Technology of India, The Digital Personal Data Protection Bill, 2022, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf; and the summary is available here: PRS Legislative Research, Draft Digital Personal Data Protection Bill, 2022, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022; and here: KPMG, Digital Personal Data Protection Bill, 2022, https://kpmg.com/in/en/home/insights/2022/12/privacy-digital-personal-data-protection-bill-2022.html

355 Text of the law is available here: Parliament of India, The Digital Personal Data Protection Act, 2023, https://egazette.gov.in/WriteReadData/2023/248045.pdf

356 D. Christopher, A. Dutta, A. Kabra, "India – The Digital Personal Data Protection Act, 2023 finally arrives", Linklaters, August 23, 2023, https://www.linklaters.com/en/insights/blogs/digilinks/2023/august/india-the-digital-personal-data-protection-act

357 Access Now, "India's Digital Personal Data Protection Bill passed: 'it's a bad law'", August 9, 2023, https://www.accessnow.org/press-release/indias-digital-personal-data-protection-bill-passed/

358 Hunton Privacy Blog, "India Passes Digital Personal Data Protection Act", Au-

gust 22, 2023, https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/

359 Text of the IT Act is available here: Parliament of India, The Information Technology Act, 2000, https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=

360 Text of the SPDI Rules is available here: Ministry of Communications and Information Technology of India, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, https://www.dataguidance.com/legal-research/information-technology-reasonable-security-practices-and-procedures-and-sensitive

361 A. Jain, P. Waghre, "IFF's first read of the draft Digital Personal Data Protection Bill, 2023", Internet Freedom Foundation, August 3, 2023, https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/; S. Saigal, "Data Protection Bill | Granting government exemption causes great concern, says Justice Srikrishna", The Hindu, July 8, 2023, https://www.thehindu.com/news/national/justice-srikrishna-on-draft-data-protection-bill-granting-govt-exemption-causes-great-concern/article67049892.ece; The Wire Staff, "Digital Personal Data Protection Bill Could Have Adverse Impact on Press Freedom, Say Editors Guild and DIGIPUB", The Wire, August 7, 2023, https://thewire.in/media/digital-personal-data-protection-bill-adverse-impact-press-freedom-editors-guild

362 Access Now, "India's Digital Personal Data Protection Bill passed: 'it's a bad law'", August 9, 2023, https://www.accessnow.org/press-release/indias-digital-personal-data-protection-bill-passed/

363 R. Roy, G. Zanfir-Fortuna, "The Digital Personal Data Protection Act of India, Explained", Future of Privacy Forum, August 15, 2023, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/

364 See Section 7(c) of the Digital Personal Data Protection Bill.

365 See Section 17 (2) (b) of the Digital Personal Data Protection Bill.

366 The Wire Staff, "Digital Personal Data Protection Bill Could Have Adverse Impact on Press Freedom, Say Editors Guild and DIGIPUB", The Wire, August 7, 2023, https://thewire.in/media/digital-personal-data-protection-bill-adverse-impact-press-freedom-editors-guild

367 S. Saigal, "Data Protection Bill | Granting government exemption causes great concern, says Justice Srikrishna", The Hindu, July 8, 2023, https://www.thehindu.com/news/national/justice-srikrishna-on-draft-data-protection-bill-granting-govt-exemption-causes-great-concern/article67049892.ece

368 Hunton Privacy Blog, "India Passes Digital Personal Data Protection Act", August 22, 2023, https://www.huntonprivacyblog.com/2023/08/22/india-passes-digital-personal-data-protection-act/

369 Text of the act is available here: Parliament of India, Criminal Procedure (Identification) Act, 2022, https://www.indiacode.nic.in/bitstream/123456789/19029/1/a2022-11_.pdf

370 A. Jain, "Delhi Police's claims that FRT is accurate with a 80% match are 100% scary", Internet Freedom Foundation, August 17, 2022, https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/

371 Z. Mateen, M. Sebastian, "CPC: Criminal Procedure Identification Bill raises fears of surveillance in India", BBC, April 13, 2022, https://www.bbc.com/news/world-asia-india-61015970

372 Unique Identification Authority of India, "What is Aadhaar", https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html

373 Daijiworld, "'Adhaar' most sophisticated ID programme in the world : World Bank", March 16, 2017, https://www.daijiworld.com/news/newsDisplay.aspx?newsID=442948

374 Money Control, "Economic Survey 2023: 135.2 crore Aadhaar numbers generated till November 2022", January 31, 2023, archived version: https://web.archive.org/web/20230131231837/https://www.moneycontrol.com/news/business/budget/economic-survey-2023-135-2-crore-aadhaar-numbers-generated-till-november-2022-9971821.html

375 Setopati, "Aadhar is constitutional but don't make it mandatory: Indian SC to govt", September 26, 2018, https://en.setopati.com/political/131199

376 Al Jazeera, "India's top court rules privacy is a fundamental right", August 24, 2017, https://www.aljazeera.com/news/2017/8/24/indias-top-court-rules-privacy-is-a-fundamental-right; BBC, "Indian Supreme Court in landmark ruling on privacy", August 24, 2017, https://www.bbc.com/news/world-asia-india-41033954

377 Pavithraa, "Aadhaar card: An Invasion to privacy", Legal Service India, https://www.legalserviceindia.com/legal/article-34-aadhaar-card-an-invasion-to-privacy.html

378 D. Dutta Roy, "Aadhaar Card Not Mandatory, Supreme Court Rules", NDTV, August 11, 2015, https://www.ndtv.com/india-news/aadhaar-card-not-mandatory-supreme-court-rules-1206134

379 Z. Saberin, "India's top court upholds constitution validity of Aadhaar card", Al Jazeera, September 26, 2018,https://www.aljazeera.com/news/2018/9/26/indias-top-court-upholds-constitution-validity-of-aadhaar-card;

Text of the judgement is available here: Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others", September 26, 2018, https://uidai.gov.in/images/Aadhaar_Judgment.pdf

380 Deccan Herald, "Aadhaar verdict: What stays, what is struck down", September 26, 2018, https://www.deccanherald.com/national/aadhaar-verdict-what-stay-what-694678.html

381 D. Grey, "SC upholds Aadhaar's Constitutional Validity, but partially addresses Privacy Concerns", CJP, September 26, 2018, https://cjp.org.in/sc-upholds-aadhaars-constitutional-validity-but-partially-addresses-privacy-concerns/

382 M. Safi, "Indian court upholds legality of world's largest biometric database", The Guardian, September 26, 2018, https://www.theguardian.com/world/2018/sep/26/indian-court-upholds-legality-of-worlds-largest-biometric-database

383 Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others", September 26, 2018, https://uidai.gov.in/images/Aadhaar_Judgment.pdf, p. 559

384 N. Nambiar, "Unique Identification Authority of India's face recognition system ready for Maharashtra's various services", The Times of India, August 20, 2022, https://timesofindia.indiatimes.com/city/pune/unique-identification-authority-of-indias-face-recognition-system-ready-for-maharashtras-various-services/articleshow/93669134.cms

385 Unique Identification Authority of India, "Resources - Videos", https://uidai.gov.in/en/media-resources/resources/videos.html

386 2021 Report on surveillance history and practices in Kenya is available here: G. Mutung'u, "Surveillance Law in Africa: a review of six countries, Kenya country report", Institute of Development Studies, 2021, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Kenya%20Country%20Report.pdf?sequence=6&isAllowed=y; and the whole report is available here: T. Roberts, "Surveillance Law in Africa: a review of six countries", Institute of Development Studies, 2021, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y

387 For surveillance during the Covid 19 pandemic, see report available here: ARTICLE 19 Eastern Africa, Kenya ICT Action Network, Pollicy, "Unseen Eyes, Unheard Stories Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19", April 21, 2021,https://www.article19.org/wp-content/uploads/2021/04/EAF-Surveillance-Report_Final-min.pdf; Surveillance of e-communications is a reason for concern, due to changes of Official Secrets Act: B. Andere, "Kenya's sneak attack on the right to privacy", Access Now, January 13, 2023,https://www.accessnow.org/kenya-right-to-privacy/

388 Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba", January 27, 2022,https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

389 Archived version of the website is available here: Huduma Namba, https://web.archive.org/web/20230510154147/https://www.hudumanamba.go.ke/

390 M. Obar, "Ruto Issues New Order Over Huduma Namba", Kenyans.co.ke, January 27, 2023,https://www.kenyans.co.ke/news/84755-ruto-makes-new-orders-over-huduma-namba

391 L. Danflow, "ICT CS Owalo: Kenyans to have digital IDs by March 2024", The Star, May 17, 2023, https://www.the-star.co.ke/news/realtime/2023-05-17-ict-cs-owalo-kenyans-to-have-digital-ids-by-march-2024/

392 D. Mwangi, "CS Kindiki reveals details of new upgraded ID cards set to be launched", Pulse, May 24, 2023, https://www.pulselive.co.ke/news/local/interior-cs-kithure-kindiki-reveals-plans-for-upgraded-identification-cards/zc8dskc

393 B. Makong, "Kenya pursues upgraded Biometric Identification System for enhanced security measures", Capital News, May 24, 2023, https://www.capitalfm.co.ke/news/2023/05/kenya-pursues-upgraded-biometric-identification-system-for-enhanced-security-measures/; M. Kinyanjui, "Kindiki: Kenyans to get ID with machine-readable chip, QR code", The Star, May 24, 2023, https://www.the-star.co.ke/news/2023-05-24-kindiki-kenyans-to-get-id-with-machine-readable-chip-qr-code/

394 M. Akuchie, "Kenya plans to tackle identity theft with an improved biometric system", Technext, May 25, 2023, https://technext24.com/2023/05/25/kenya-identity-theft-biometric/

395 D. Mwangi, "CS Kindiki reveals details of new upgraded ID cards set to be launched", Pulse, May 24, 2023, https://www.pulselive.co.ke/news/local/interior-cs-kithure-kindiki-reveals-plans-for-upgraded-identification-cards/zc8dskc

396 J. Thiong'o, "Inside President Ruto's bid to ditch Huduma Namba, adopt Digital Identity project", The Standard, June 1, 2023, https://www.standardmedia.co.ke/article/2001474305/inside-president-rutos-bid-to-ditch-huduma-namba-adopt-identity-project

397 P. Wanjama, "Police Launch Facial Recognition System to Nab Criminals", Kenyans.co.ke, September 18, 2018, https://www.kenyans.co.ke/news/33249-police-launch-facial-recognition-system-nab-criminals; C. Burt, "Kenyan police launch facial recognition on urban CCTV network", Biometric Update, September 24, 2018, https://www.biometricupdate.com/201809/kenyan-police-launch-facial-recognition-on-urban-cctv-network; Business Today Kenya, "Big brother gets bigger: Police acquire face recognition capabilities", September 18, 2018, https://businesstoday.co.ke/big-brother-gets-bigger-police-acquire-face-recognition-capabilities/

398 According to the report available here: INCLO, "In Focus Facial Recognition Tech Stories And Rights Harm Around The World", January 2021, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

399 C. Burt, "NEC facial recognition border tech for Kenya as airport biometrics rollouts continue", Biometric Update, October 7, 2019, https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrics-rollouts-continue; International Organization for Migration, "Facial Recognition System Installed at Moi International Airport", October 7, 2019, https://www.iom.int/news/facial-recognition-system-installed-moi-international-airport

400 F. Hersey, "850 Kenyan hospitals sue national insurance fund over biometric patient registration", Biometric Update, August 4, 2021, https://www.biometricupdate.com/202108/850-kenyan-hospitals-sue-national-insurance-fund-over-biometric-patient-registration; L. Igadwah, "850 private hospitals sue NHIF in biometric registration dispute", Business Daily, August 3, 2021, https://www.businessdailyafrica.com/bd/economy/rural-based-hospitals-sue-nhif-biometric-registration-dispute-3496384

401 E. Weiss, "Kenya Replaces Insurance Cards With Fingerprint Biometrics", FindBiometrics, July 9, 2021, https://findbiometrics.com/kenya-replaces-insurance-cards-with-fingerprint-biometrics-070904/; B. Otieno, "Uhuru launches biometric Universal Health Coverage registration", The Star, October 31, 2020, https://www.the-star.co.ke/news/2020-10-31-uhuru-launches-biometric-universal-health-coverage-registration/; A. Macdonald, "Biometric registration drive in Kenya for health insurance scheme", Biometric Update, June 15, 2021, https://www.biometricupdate.com/202106/biometric-registration-drive-in-kenya-for-health-insurance-scheme

402 S. Kiplagat, "Safaricom and Airtel want enjoined in fresh SIM cards registration case", Business Daily, April 6, 2022, https://www.businessdailyafrica.com/bd/corporate/companies/safaricom-and-airtel-want-enjoined-sim-cards-registration-case-3773596; C. Burt, "Subscribers scramble for biometric SIM

registrations in Kenya as deadline extended", Biometric Update, April 20, 2022,https://www.biometricupdate.com/202204/subscribers-scramble-for-biometric-sim-registrations-in-kenya-as-deadline-extended

403 Access Now, "Open letter: Safaricom must delete all biometric data collected unlawfully during Kenya's SIM card registration exercise", December 14, 2022,https://www.accessnow.org/press-release/open-letter-safaricom-privacy-kenya/

404 Text of the Constitution is available here: Constitution of Kenya, 2010,http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010

405 Text of the KDPA in English is available here: Parliament of Kenya, The Data Protection Act, 2019, https://www.odpc.go.ke/dpa-act/

406 DLA Piper, "Global Data Protection Laws of the World - Kenya", January 12, 2023,https://www.dlapiperdataprotection.com/index.html?t=law&c=KE

407 Website in English is available here: Office of the Data Protection Commissioner of Kenya, https://www.odpc.go.ke/

408 Issued guidelines are available here: Office of the Data Protection Commissioner of Kenya, "General Guidelines", https://www.odpc.go.ke/general-guidlines/

409 Detailed review of the legal framework of Kenya is available here: R. Reeve et al., "Data Privacy and Protection in Kenya: A Regulatory Review", FSD Kenya, January 2022, https://www.fsdkenya.org/wp-content/uploads/2022/01/Dapa-January-26th.pdf

410 All Regulations are available in English here: Office of the Data Protection Commissioner of Kenya, "Data Protection Regulations", https://www.odpc.go.ke/data-protection-regulation/

411 Article 13 and Third Schedule of Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021. There is a publicly available registry with mandatory registrations, but it contains only the basic details about registered controllers and processors and not the type of registered processing activities. The public register is available here: Office of the Data Protection Commissioner of Kenya, "Register Of Data Controllers And Data Processors", https://www.odpc.go.ke/registered-data-processors-and-controllers/

412 Article 46 of the KDPA specifically regulates only the processing of health data.

413 Transfer of data, including sensitive data, is in detail regulated in the Part II of the Data Protection (General) Regulations, 2021.

414 These are primarily contained in Article 28(2) of the KDPA that regulates the situations in which data can be collected indirectly, which are when: (a) the data is contained in a public record; (b) the data subject has deliberately made the data public; (c) the data subject or his or her guardian has consented to the collection from another source; (d) the collection from another source would not prejudice the interests of the data subject; and (e) collection of data from another source is necessary: (i) for the prevention, detection, investigation, prosecution and punishment of crime; (ii) for the enforcement of a law which imposes a pecuniary penalty; or (iii) for the protection of the interests of the data subject or another person.

415 Article 6(1)(e) of the Data Protection (General) Regulations, 2021.

416 Published Guidelines available here: Office of the Data Protection Commissioner of Kenya, "General Guidelines", https://www.odpc.go.ke/general-guidlines/

417 The history of the legal procedures can be found here: Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba", January 27, 2022, https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

418 Text of the judgement in English is available here: High Court of Kenya at Nairobi, "Nubian Rights Forum & 2 others v. Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR", January 30, 2020, http://kenyalaw.org/caselaw/cases/view/189189/

419 See paragraphs 781, 784, 910, 919, 922 and 1038 of the judgement. More details about the judgement can be found here: Privacy International, "Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons", February 24, 2020, https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

420 See paragraph 1047 of the judgement. The court ruled, inter alia, on the constitutionality and legality of measures related to public participation in the legislative process; on whether there is violation of the right to privacy (whether the personal information collected is excessive, intrusive, and disproportionate, whether there is a violation of children's rights to privacy, whether there are sufficient legal safeguards and data protection frameworks); and whether there was a violation of the right to equality and non-discrimination.

421 Text of the judgement in English can be found here: High Court of Kenya at Nairobi (Milimani Law Courts), "Republic v. Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party) (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review)", October 14, 2021, http://kenyalaw.org/caselaw/cases/view/220495/; Analysis of the judgement: Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba", January 27, 2022, https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma; Media Defence, "Advanced Modules on Digital Rights and Freedom of Expression Online in sub-Saharan Africa, Module 4: Privacy and Security Online, Collection of Biometric Data and Facial Recognition", https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/collection-of-biometric-data-and-facial-recognition/; The Open Society Justice Initiative, "New Kenya High Court Judgment Sets Important Precedent for Digital ID Privacy Protections and Processes", October 15, 2021, https://www.justiceinitiative.org/newsroom/new-kenya-high-court-judgment-sets-important-precedent-for-digital-id-privacy-protections-and-processes

422 See paragraph 104 of the judgement.

423 See paragraph 119 of the judgement.

424 A. Macdonald, "Kenya mulls digital ID scheme changes and new uses for con-

troversial Huduma Namba", Biometric Update, January 16, 2023, https://www.biometricupdate.com/202301/kenya-mulls-digital-id-scheme-changes-and-new-uses-for-controversial-huduma-namba

425 A. Macdonald, "Activists urge Kenya not to repeat mistakes of Huduma Namba in new digital ID plan", Biometric Update, May 22, 2023, https://www.biometricupdate.com/202305/activists-urge-kenya-not-to-repeat-mistakes-of-huduma-namba-in-new-digital-id-plan

426 Office of the Data Protection Commissioner of Kenya, "Office of the Data Protection Commissioner Issues a Penalty Notice against Oppo Kenya", January 28, 2023, https://www.odpc.go.ke/download/office-of-the-data-protection-commissioner-issues-a-penalty-notice-against-oppo-kenya/; G. Ndung'u, A. Issaias,T. Mwango, "Kenya: The Office of the Data Protection Commissioner issues decisions in the determination of complaints", Bowmans, January 19, 2023, https://bowmanslaw.com/insights/data-protection/kenya-the-office-of-the-data-protection-commissioner-issues-decisions-in-the-determination-of-complaints/

427 M. Badillo, "Navigating the complexities of facial recognition for public security in Latin America", International Bar Association, May 9, 2023, https://www.ibanet.org/facial-recognition-security-latin-america

428 Access Now, "Made Abroad, Deployed at Home", August 2021, https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

429 C. Caeiro, "Regulating facial recognition in Latin America", Chatham House, November 11, 2022, https://www.chathamhouse.org/2022/11/regulating-facial-recognition-latin-america

430 J. Ramos, "Latin Americans Are Furious", The New York Times, November 8, 2019,https://www.nytimes.com/2019/11/08/opinion/contributors/latin-america-protest-repression.html

431 F. Fascendini, F. Roveri, "Your software is my biology: The mass surveillance system in Argentina", Global Information Society Watch (GISWatch), 2014, https://giswatch.org/en/country-report/communications-surveillance/argentina

432 Ibid.

433 Área Digital Asociación por los Derechos Civiles, "Cuantificando identidades en América Latina", May 2017, https://adc.org.ar/wp-content/uploads/2019/06/029-cuantificando-identidades-en-america-latina-05-2017.pdf (in Spanish)

434 D. Gershgorn, "The US Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life", OneZero, March 4, 2020, https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d

435 European Digital Rights (EDRi), "Dangerous by design: A cautionary tale about facial recognition", February 12, 2020, https://edri.org/our-work/dangerous-by-design-a-cautionary-tale-about-facial-recognition/

436 M. Badillo, "Judge declares Buenos Aires' Fugitive Facial Recognition System Unconstitutional", Future of Privacy Forum, September 30, 2022, https://fpf.org/blog/judge-declares-buenos-aires-fugitive-facial-recognition-system-unconstitutional/

437 A. Mascellino, "Brazil deploys ISS facial recognition to secure São Paulo metro", Biometric Update, December 9, 2022, https://www.biometricupdate.com/202212/brazil-deploys-iss-facial-recognition-to-secure-sao-paulo-metro

438 A. Makoni, "Brazil's Embrace Of Facial Recognition In Schools Is Worrying Its Black Communities", POCIT, May 17, 2022, https://peopleofcolorintech.com/general/brazils-embrace-of-facial-recognition-in-schools-is-worrying-black-communities/

439 DataGuidance, "Brazil: ViaQuatro is fined BRL 100,000 for improper facial recognition practices at subway stations", May 11, 2021, https://www.dataguidance.com/news/brazil-viaquatro-fined-brl-100000-improper-facial

440 M. Garrote, N. Paschoalini, M. Meira, "Why should we all pay attention to the Brazilian Digital ID system?", Data Privacy Brasil Research Association, November 23, 2022, https://www.dataprivacybr.org/why-should-we-all-pay-attention-to-the-brazilian-digital-id-system-2/

441 B. Bioni et al., "Between visibility and exclusion: mapping the risks associated with the National Civil Identification System and the usage of its database by the gov.br platform", Data Privacy Brasil Research Association, 2022, https://www.dataprivacybr.org/wp-content/uploads/2022/11/Policy-paper-Data-Privacy-Brazil-Research-BETWEEN-VISIBILITY-AND-EXCLUSION.pdf

442 Access Now, "Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data", March 23, 2023, https://www.accessnow.org/press-release/statement-terminate-agreements-biometric-data-migrants/

443 C. Caeiro, "06 To ban or to regulate facial recognition in Latin America? The debate", Chatham House, November 11, 2022, https://www.chathamhouse.org/2022/11/regulating-facial-recognition-latin-america/06-ban-or-regulate-facial-recognition-latin

444 Referenced before, this part is in the conclusion: Access Now, "Made Abroad, Deployed at Home", August 2021, https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

445 Coding Rights, "Legislators from all regions of Brazil present bills to ban facial recognition in public spaces", June 22, 2022, https://medium.com/codingrights/legislators-from-all-regions-of-brazil-present-bills-to-ban-facial-recognition-in-public-spaces-31d8da0d3822

446 DLA Piper, "Global Data Protection Laws of the World - Chile", January 28, 2023, https://www.dlapiperdataprotection.com/index.html?t=law&c=CL

447 Guyer & Regules, "Global Data Protection Law Guide - Uruguay", Multilaw, 2023, https://www.multilaw.com/Multilaw/Data_Protection_Laws_Guide/DataProtection_Guide_Uruguay.aspx

448 DLA Piper, "Global Data Protection Laws of the World - Mexico", January 12, 2023, https://www.dlapiperdataprotection.com/index.html?t=law&c=MX

449 DLA Piper, "Global Data Protection Laws of the World - Costa Rica", January 26, 2023, https://www.dlapiperdataprotection.com/index.html?t=law&c=CR

450 B. Fernandez Nieto, "Habeas Data and Personal Data Protection in Latin America", Data-Pop Alliance, August 25, 2022, https://datapopalliance.org/habeas-data-and-personal-data-protection-in-latin-america/

451 AlSur, "Facial recognition in Latin America", 2021, https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf

452 Ministério dos Transportes do Brasil, Portaria Denatran N° 1515, 2018, https://www.legisweb.com.br/legislacao/?id=372479 (in Portuguese)

453 Legislatura de la Ciudad Autónoma De Buenos Aires, Sistema Integral De Seguridad Pública De La Ciudad Autónoma De Buenos Aires, Ley Q - N° 5.688, 2016, https://digesto.buenosaires.gob.ar/documento/download/Ley%20Ciudad-5688__68dc0cdd582d3dd01f4f976a796c5cda9d7ab7dd.pdf (in Spanish)

454 Congreso de la República de Colombia, Código Electoral Colombiano, PL 234-20, 2020, http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2020-2021/2021-proyecto-de-ley-234-de-2020 (in Spanish)

455 Constitution for the Argentine Nation, http://www.biblioteca.jus.gov.ar/argentina-constitution.pdf

456 Congress of the Argentine Nation, Act 25.326, 2000, http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf

457 Télam, "La Legislatura aprobó el uso de reconocimiento facial para la detención de prófugos", October 22, 2020, https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html (in Spanish)

458 Diario Judicial, "Sonría, lo estamos filmando", October 22, 2020, https://www.diariojudicial.com/news-87691-sonria-lo-estamos-filmando (in Spanish)

459 OHCHR, "Statement to the media by the United Nations Special Rapporteur on the right to privacy, on the conclusion of his official visit to Argentina, 6-17 May 2019", May 23, 2019, https://www.ohchr.org/en/statements/2019/05/statement-media-united-nations-special-rapporteur-right-privacy-conclusion-his

460 E. Ferreyra, "Facial recognition in Latin America: Towards a human rights-based legal framework to protect public spaces from mass surveillance", Global Campus of Human Rights, 2020, https://repository.gchumanrights.org/items/b6fb1ba9-95d2-436a-a4ef-a2471b54a9cf

461 M. Peruzzotti, "Argentina: Draft bill on personal data protection", IAPP, October 28, 2022, https://iapp.org/news/a/argentina-draft-bill-on-personal-data-protection/

462 Agencia de Acceso a la Información Pública de Argentina, Resolución 4/2019, 2019, https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm (in Spanish)

463 Privacy International, "Privacy International's submission Argentina's draft law on the protection of personal data, 2022", September 2022, https://privacyinternational.org/sites/default/files/2022-11/PI%20comments%20on%20Propuesta%20de%20anteproyecto%20de%20ley%202022.pdf

464 Constitution of the Federative Republic of Brazil, 3rd Edition, 2010, https://www.globalhealthrights.org/wp-content/uploads/2013/09/Brazil-constitution-English.pdf

465 Presidency of Brazil, Marco Civil Law of the Internet in Brazil, Law No. 12.965, 2014, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

466 National Congress of Brazil, Brazilian Data Protection Law (LGPD), as amended by Law No. 13.853, 2019, https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

467 DataGuidance, "Brazil: House of Representatives approves constitutional amendment on the protection of personal data", September 1, 2021, https://www.dataguidance.com/news/brazil-house-representatives-approves-constitutional

468 Câmara dos Deputados, "Exposição de Motivos: Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal", 2019, https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/outros-documentos/DADOSAnteprojetocomissaoprotecaodadosseguran-capersecucaoFINAL.pdf (in Portuguese)

469 Assembléia Legislativa do Ceará, Lei N.º 16.873, 2019, https://belt.al.ce.gov.br/index.php/legislacao-do-ceara/organizacao-tematica/cultura-e-esportes/item/6638-lei-n-16-873-de-10-05-19-d-o-10-05-19 (in Portuguese)

470 Assembléia Legislativa de Minas Gerais, Lei Nº 21737, 2015, https://www.legisweb.com.br/legislacao/?id=287944 (in Portuguese)

471 Assembléia Legislativa de Alagoas, Lel Nº 8.113, 2019, https://sapl.al.al.leg.br/media/sapl/public/normajuridica/2019/1594/lei_no_8.113_de_29.05.2019.pdf

472 Assembléia Legislativa do Estado do Rio de Janeiro, Lei Nº 7123, 2015, https://www.legisweb.com.br/legislacao/?id=384128 (in Portuguese)

473 Câmara Legislativa do Distrito Federal, Lei Nº 6.712, 2020, https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf (in Portuguese)

474 E. Sakiotis et al., "Brazil's Senate Committee Publishes AI Report and Draft AI Law", Covington Inside Privacy, January 27, 2023, https://www.insideprivacy.com/emerging-technologies/brazils-senate-committee-publishes-ai-report-and-draft-ai-law/

475 K. Silva, "Brazilian court declares data protection a fundamental right in landmark decision", Global Data Review, May 11, 2020, https://globaldatareview.com/article/brazilian-court-declares-data-protection-fundamental-right-in-landmark-decision

476 Access Now, "Privacy win for 350,000 people in São Paulo: court blocks facial recognition cameras in metro", May 12, 2021, https://www.accessnow.org/press-release/sao-paulo-court-bans-facial-recognition-cameras-in-metro/

477 Global Freedom of Expression, "The Case of São Paulo Subway Facial Recognition Cameras", Global Freedom of Expression, May 7, 2021, https://globalfreedomofexpression.columbia.edu/cases/the-case-of-sao-paulo-subway-facial-recognition-cameras/

478 M. Badillo, "Judge declares Buenos Aires' Fugitive Facial Recognition System Unconstitutional", Future of Privacy Forum, September 30, 2022, https://fpf.org/blog/judge-declares-buenos-aires-fugitive-facial-recognition-system-un-

constitutional/

479 C. Garrison, V. Hilaire, "Mexico's top court strikes down controversial cell-phone registry with biometric data", Reuters, April 25, 2022, https://www.reuters.com/world/americas/mexicos-top-court-strikes-down-creation-cell-phone-registry-with-biometric-user-2022-04-25/

480 H. Swart, "Face-off: South Africa's population register is on course to becoming a criminal database – with your mugshot", Daily Maverick, March 3, 2021, https://www.dailymaverick.co.za/article/2021-03-03-face-off-south-africas-population-register-is-on-course-to-becoming-a-criminal-database-with-your-mugshot/

481 K. Hao, H. Swart, "South Africa's private surveillance machine is fueling a digital apartheid", MIT Technology Review, April 19, 2022, https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/; M. Kwet, "Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa", Vice, November 22, 2019, https://www.vice.com/en/article/pa7nek/smart-cctv-networks-are-driving-an-ai-powered-apartheid-in-south-africa; S. Mungadze, "Professor decries Joburg's private surveillance networks", ITWeb, September 3, 2019, https://www.itweb.co.za/content/Pero37ZgoYJMQb6m; K. Allen, I. van Zyl, "Who's watching who? Biometric surveillance in Kenya and South Africa", ENACT, November 2020, https://enact-africa.s3.amazonaws.com/site/uploads/2020-11-11-biometrics-research-paper.pdf; H. Swart, A. Munoriyarwa, "Video Surveillance in Southern Africa: Case studies of security camera systems in the region", Media Policy and Democracy Project, May 2020, https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

482 Department of Home Affairs of South Africa, "What is ABIS?", http://www.dha.gov.za/index.php/civic-services/abis

483 BusinessTech, "Home Affairs proposes big change for IDs in South Africa", August 26, 2022, https://businesstech.co.za/news/government/620051/home-affairs-proposes-big-change-for-ids-in-south-africa/

484 A. Macdonald, "Delays persist in South Africa's automated biometric identification project completion", Biometric Update, March 16, 2021, https://www.biometricupdate.com/202103/delays-persist-in-south-africas-automated-biometric-identification-project-completion; M. Illidge, "The truth about South Africa's undelivered R432-million biometrics database", MyBroadband, September 12, 2022, https://mybroadband.co.za/news/government/460005-the-truth-about-south-africas-undelivered-r432-million-biometrics-database.html

485 Parliament of South Africa, "Media Statement: Home Affairs Committee Disappointed With Lack of Progress in Migrating to Automated Biometric Identification System", May 10, 2023, https://www.parliament.gov.za/press-releases/media-statement-home-affairs-committee-disappointed-lack-progress-migrating-automated-biometric-identification-system

486 S. Mzekandaba, "Home affairs ramps up biometrics-driven movement system", ITWeb, May 9, 2023, https://www.itweb.co.za/content/o1Jr5MxPKNBMKdWL; A. Macdonald, "South Africa to expand biometric border control system", Biometric Update, May 11, 2023, https://www.biometricupdate.com/202305/south-africa-to-expand-biometric-border-control-system;

487 This announcement is available here: Department of Home Affairs of South Africa, "Biometrics capturing process", https://www.flysaa.com/documents/51855150/0/Biometrics+Poster+without+bleeds.pdf/ba8a9b4a-e5dc-4569-8ea3-31220aad2631

488 Article 14 of Constitution of the Republic of South Africa, 1996, available here: Constitution of the Republic of South Africa, Chapter 2: Bill of Rights, 1996, https://www.gov.za/documents/constitution/chapter-2-bill-rights#14; South Africa is a party to the International Covenant on Civil and Political Rights (ICCPR).

489 Text in English available here: Parliament of South Africa, Protection of Personal Information Act (POPIA) 4 of 2013, https://www.gov.za/documents/protection-personal-information-act

490 Website in English is available here: Information Regulator South Africa, https://inforegulator.org.za/; This body acts also as competent authority in the area of access to public information.

491 Articles 26 and 27 of POPIA.

492 According to the definition from POPIA, "responsible party" corresponds to the definition of "controller" from the GDPR, and means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

493 Available here: Information Regulator South Africa, "Guidance Notes", https://inforegulator.org.za/guidance-notes/

494 Article 33 of POPIA.

495 It may be worth noting that South Africa does have a law that regulates interception of communication, Regulation of Interception of Communications and Provision of Communications Related Information Act (2002), available here: Parliament of South Africa, Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, https://www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13; This regulates that law enforcement should apply for judicial authorisation for the interception of communications.

496 Available here: Information Regulator South Africa, "Prior Authorisation", https://inforegulator.org.za/prior-authorisation/

497 Facts and the law are summarised here: S. de Gouveia, K. Robertson, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others", Schindlers Attorneys September 1, 2020, https://www.schindlers.co.za/2020/vumacam-pty-ltd-v-johannesburg-roads-agency-and-others/; and here: J. Nash, "A 2020 court fight in South Africa reveals dominance of biometric surveillance industry", Biometric Update, April 21, 2022, https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry; and the High Court decision can be found here: South Gauteng High Court, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186", August 20, 2020, http://www.saflii.org/za/cases/ZAGPJHC/2020/186.html

498 Judgement, paras 6 and 7: South Gauteng High Court, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186", August 20, 2020, http://www.saflii.org/za/cases/ZAGPJHC/2020/186.html

499 Judgment, para 16: South Gauteng High Court, "Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186", August 20, 2020, http://www.saflii.org/za/cases/ZAGPJHC/2020/186.html

500 The Article with the interview is available here: S. Mungadze, "Johannesburg Road Agency loses CCTV court appeal", ITWeb, October 5, 2020, https://www.itweb.co.za/content/kYbe97XDrV27AWpG

501 Xische & Co, "The UAE Can Lead in Facial Recognition", May 26, 2021, https://www.xische.com/all-articles/2019/7/01/the-uae-can-lead-in-facial-recognition

502 M. Rajagopalan, "IBM, Huawei, And Hikvision Are Battling To Sell Facial Recognition Technology In Dubai", Buzzfeed News, May 29, 2019, https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

503 Minister of State for Artificial Intelligence, Digital Economy & Remote Work Applications Office, UAE National Strategy for Artificial Intelligence 2031, https://ai.gov.ae/strategy/

504 Ibid.

505 UAE PASS, "About", https://selfcare.uaepass.ae/about

506 UAE PASS, https://selfcare.uaepass.ae/

507 Ministry of Cabinet Affairs, "UAE Government to employ biometric face recognition to register customers under 'UAE Pass' app", April 7, 2021, https://www.moca.gov.ae/en/media/news/uae-government-to-employ-biometric-face-recognition-to-register-customers-under-%27uae-pass%27-app

508 Ibid.

509 Z. Husain, "UAE: Facial recognition instead of Emirates ID card readers will now verify identity", Gulf News, October 19, 2021, https://gulfnews.com/living-in-uae/ask-us/uae-facial-recognition-instead-of-emirates-id-card-readers-will-now-verify-identity-1.1634628283290; Z. Husain, "UAE: Three ways you can access the digital version of your Emirates ID for free", Gulf News, February 9, 2023, https://gulfnews.com/living-in-uae/visa-immigration/uae-three-ways-you-can-access-the-digital-version-of-your-emirates-id-for-free-1.1675855637719

510 Dubai Police, Facebook, October 30, 2021, https://www.facebook.com/dubaipolicehq.en/photos/a.136978203046390/4512542835489883/?type=3; Khaleej Times, "Dubai Police to launch AI-enabled platform for decision-making process", October 30, 2021, https://www.khaleejtimes.com/uae/dubai-police-to-launch-ai-enabled-platform-for-decision-making-process

511 The Official Portal of the UAE Government, "Maintaining safety and security", https://u.ae/en/information-and-services/justice-safety-and-the-law/maintaining-safety-and-security

512 Dubai Police, Facebook, January 27, 2018, https://www.facebook.com/dubaipolicehq.en/videos/1600201106724085/; P. Bhunia, "Dubai Police launches artificial intelligence-based surveillance programme", OpenGov Asia, January 29, 2018, https://opengovasia.com/dubai-police-launches-artificial-intelligence-based-surveillance-programme/; M. Rajagopalan, "IBM, Huawei, And Hikvision Are Battling To Sell Facial Recognition Technology In Dubai", Buzzfeed News, May 29, 2019, https://www.buzzfeednews.com/arti-

cle/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

513 A. Al Shouk, "How Dubai's AI cameras helped arrest 319 suspects last year", Gulf News, March 18, 2019, https://gulfnews.com/amp/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675

514 City Security Magazine, "Dubai Police take personal security to a whole new level", September 12, 2022, https://citysecuritymagazine.com/editors-choice/dubai-police-take-personal-security-to-a-whole-new-level; Gulf Business, "Dubai monitored by 300,000 cameras, one of the world's safest cities - Sheikh Mohammed", July 14, 2021, https://gulfbusiness.com/dubai-monitored-by-300000-cameras-one-of-the-worlds-safest-cities-sheikh-mohammed/; B. Sapra, "Dubai police unveil plan to use drones", WIRED Middle East, July 14, 2021, https://wired.me/technology/dubai-police-unveil-plan-to-use-drones/

515 A. Al Shouk, "Watch: Facial recognition at Dubai Metro stations to identify wanted criminals", Gulf News, November 22, 2020, https://gulfnews.com/uae/government/watch-facial-recognition-at-dubai-metro-stations-to-identify-wanted-criminals-1.75309516

516 L. Pascu, "Abu Dhabi police upgrade patrol cars with live biometric facial recognition", Biometric Update, March 19, 2020, https://www.biometricupdate.com/202003/abu-dhabi-police-upgrade-patrol-cars-with-live-biometric-facial-recognition; A. Kumar, "These patrol cars can soon spot criminals on UAE streets", Khaleej Times, March 10, 2020, https://www.khaleejtimes.com/uae/these-patrol-cars-can-soon-spot-criminals-on-uae-streets

517 M. Rajagopalan, "IBM, Huawei, And Hikvision Are Battling To Sell Facial Recognition Technology In Dubai", Buzzfeed News, May 29, 2019, https://www.buzzfeednews.com/article/meghara/dubai-facial-recognition-technology-ibm-huawei-hikvision

518 J. Lynch, "Iron net: Digital repression in the Middle East and North Africa", European Council on Foreign Relations, June 19, 2022, https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/

519 Article 36 of the Constitution, available in English here: Constitution of the United Arab Emirates, https://www.wipo.int/edocs/lexdocs/laws/en/ae/ae030en.pdf

520 Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, available in Arabic here: UAE Government, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, 2021, https://u.ae/-/media/Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.ashx (in Arabic); Text of the PDPL is not publicly available in English, but some useful overviews are: DLA Piper, "Data Protection Laws of the World UAE - General", 2023, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=AE; Al Tamimi & Co, "UAE's New Federal Data Protection Law", December 6, 2021, https://www.tamimi.com/news/uaes-new-federal-data-protection-law/; R. Rizvi, "UAE - Data Protection Overview", DataGuidance, April 2023, https://www.dataguidance.com/notes/uae-data-protection-overview

521 The Official Portal of the UAE Government, "Data protection laws", https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

522 Al Tamimi & Co, "UAE's New Federal Data Protection Law", December 6,

2021, https://www.tamimi.com/news/uaes-new-federal-data-protection-law/

523 R. Rizvi, "UAE - Data Protection Overview", DataGuidance, April 2023, https://www.dataguidance.com/notes/uae-data-protection-overview

524 Article 10 of the PDPL: UAE Government, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, 2021, https://u.ae/-/media/Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.ashx (in Arabic)

525 Article 21 of the PDPL: UAE Government, Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data, 2021, https://u.ae/-/media/Documents-2023/ArFederal-Decree-Law-No-45-of-2021-regarding-the-Protection-of-Personal-Data.ashx (in Arabic)

526 House of Lords of the United Kingdom, "Attorney General's Reference No. 3 of 1999", December 14, 2000, https://publications.parliament.uk/pa/ld200001/ldjudgmt/jd001214/agref-1.htm

527 Statewatch, "UK: Police can keep DNA of innocent people indefinitely", March 28, 2012, https://www.statewatch.org/news/2004/september/uk-police-can-keep-dna-of-innocent-people-indefinitely/

528 P. Fussey, W. Webster, "Interim report on the Abolition of the Office of the Biometrics and Surveillance Camera Commissioner as proposed by the UK Data Protection and Digital Information Bill", Centre for Research into Information, Surveillance and Privacy (CRISP), May 11, 2023, http://www.crisp-surveillance.com/blog/233253/interim-report-abolition-office-biometrics-and-surveillance-camera-commissioner-proposed

529 V. Dodd, "Met police to use facial recognition software at Notting Hill carnival", The Guardian, August 5, 2017, https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival

530 UK Information Commissioner's Office, "Information Commissioner's Opinion: The use of live facial recognition technology in public places", June 18, 2021, https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

531 Privacy International, "Civil Society Groups: Live Facial Recognition Technology should not be used in public spaces", August 2021, https://privacyinternational.org/sites/default/files/2021-08/LFRT Open Letter Final.pdf

532 P. Collings, M. Guariglia, "Ban Government Use of Face Recognition In the UK", Electronic Frontier Foundation, September 26, 2022, https://www.eff.org/deeplinks/2022/09/ban-government-use-face-recognition-uk

533 M. Ryder, "The Ryder Review", Ada Lovelace Institute, June 2022, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf

534 Parliament of the United Kingdom, Human Rights Act 1998, https://www.legislation.gov.uk/ukpga/1998/42/contents

535 Government of the United Kingdom, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, https://www.legislation.gov.uk/uksi/2019/419/contents/made

536 Parliament of the United Kingdom, Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

537 Scottish Biometrics Commissioner, "What are biometrics?", https://www.biometricscommissioner.scot/biometrics/what-are-biometrics/

538 UK Information Commissioner's Office, "Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places", October 31, 2019, https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

539 UK Information Commissioner's Office, "The use of live facial recognition technology in public places", June 18, 2021, https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

540 Parliament of the United Kingdom, Police and Criminal Evidence Act 1984, https://www.legislation.gov.uk/ukpga/1984/60/contents

541 Parliament of the United Kingdom, Terrorism Act 2000, https://www.legislation.gov.uk/ukpga/2000/11/contents

542 Parliament of the United Kingdom, Protection of Freedoms Act 2012, https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

543 S. Rowe, J. Jones, "The Biometrics and Surveillance Camera Commissioner: streamlined or eroded oversight?", Ada Lovelace Institute, October 9, 2020, https://www.adalovelaceinstitute.org/blog/biometrics-surveillance-camera-commissioner/

544 Scottish Parliament, Scottish Biometrics Commissioner Act 2020, https://www.legislation.gov.uk/asp/2020/8/contents

545 Scottish Biometrics Commissioner, "Code of Practice", November 2022, https://www.biometricscommissioner.scot/media/5y0dmsq3/biometrics-code-of-practice.pdf

546 European Court of Human Rights, "Case of S. and Marper v. the United Kingdom", December 4, 2008, https://rm.coe.int/168067d216

547 England and Wales Court of Appeal, "R (Bridges) v. Chief Constable of South Wales Police", August 11, 2020, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

548 UK Supreme Court, "Bank Mellat v. HM Treasury", June 19, 2013, https://www.supremecourt.uk/cases/uksc-2011-0040.html

549 Monitoring tool with the map: Fight for the Future, "Ban Facial Recognition", https://www.banfacialrecognition.com/map/

550 N. Turner Lee, C. Chin, "Police surveillance and facial recognition: Why data privacy is imperative for communities of color", The Brookings Institution, April 12, 2022, https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/; R. Brandom, "Most US government agencies are using facial recognition", The Verge, August 25, 2021, https://www.theverge.com/2021/8/25/22641216/facial-recognition-gao-report-agency-dhs-cbp-fbi; Mordor Intelligence, "United States Facial Recognition Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028)", https://www.mordorintelligence.com/industry-reports/united-states-facial-recognition-market

551 NYCLU, "What You Need to Know About New York's Temporary Ban on Facial Recognition in Schools", July 2, 2021, https://www.nyclu.org/en/publications/what-you-need-know-about-new-yorks-temporary-ban-facial-recognition-schools

552 Proposed in Massachusetts: Massachusetts General Court, Bill H.142, An Act establishing the Massachusetts Information Privacy Act, 2021, https://malegislature.gov/Bills/192/H142

553 Please see below Section on Vermont.

554 Some proposals can be found: Y. D. Clarke, "Reps. Clarke, Pressley & Tlaib Announce Bill to Ban Public Housing Usage of Facial Recognition & Biometric Identification Technology", Clarke.Senate.gov, https://clarke.house.gov/nobiometricsbarriers/; D. Beyer, "Beyer, Lieu Reintroduce Legislation To Block Law Enforcement From Using Facial Recognition Technology With Body Cam Footage", Beyer.House.gov, June 21, 2022, https://beyer.house.gov/news/documentsingle.aspx?DocumentID=5619; C. Coons, "Facial recognition tech: Sens. Coons, Lee bill requires court orders for law enforcement use of facial recognition technology", Coons.Senate.gov, November 14, 2019, https://www.coons.senate.gov/news/press-releases/facial-recognition-tech-sens-coons-lee-bill-requires-court-orders-for-law-enforcement-use-of-facial-recognition-technology

555 2021 proposal is available: United States Congress, S.2052 - Facial Recognition and Biometric Technology Moratorium Act of 2021, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2052?s=1&r=1&q=%7B%22search%22%3A%5B%22Facial+Recognition+and+Biometric+Technology-+Moratorium+Act+of+2021%22%5D%7D

556 Text of the proposal is available: United States Congress, Facial Recognition and Biometric Technology Moratorium Act of 2023, https://www.markey.senate.gov/imo/media/doc/facial_recognition_and_biometric_technology_moratorium_act_-_2023.pdf

557 Summary and statements: E. Markey, "Markey, Merkley, Jayapal Lead Colleagues on Legislation to Ban Government Use of Facial Recognition and Other Biometric Technology", Markey.Senate.gov, March 7, 2023, https://www.markey.senate.gov/news/press-releases/markey-merkley-jayapal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology; J. Lyons Hardcastle, "Law bill seeks to ban Feds' use of facial recognition tech", The Register, March 7, 2023, https://www.theregister.com/2023/03/07/us_ban_facial_recognition; A. Passett, "US Congress Members Reintroduce Serious Facial Recognition Bill", TechZone360, March 8, 2023, https://www.techzone360.com/topics/techzone/articles/2023/03/08/455203-us-congress-members-reintroduce-serious-facial-recognition-bill.htm

558 Text of the proposal is available here: United States Congress, H. R. 9061, 2022, https://www.congress.gov/bill/117th-congress/house-bill/9061/text?s=1&r=9

559 J. Laperruque, "The Facial Recognition Act: A Promising Path to Put Guardrails on a Dangerously Unregulated Surveillance Technology", Lawfare, November 1, 2022, https://www.lawfareblog.com/facial-recognition-act-promising-path-put-guardrails-dangerously-unregulated-surveillance-technology

560 CaseGuard, "The Facial Recognition Act of 2022, New Proposed Law", Oc-

tober 28, 2022, https://caseguard.com/articles/the-facial-recognition-act-of-2022-new-proposed-law/

561 J. Laperruque, "Limiting Face Recognition Surveillance: Progress and Paths Forward", Center for Democracy and Technology, August 23, 2022, https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward/

562 This taxonomy is available: A. Kak, "Regulating Biometrics: Global Approaches and Open Questions", AI Now Institute, September 1, 2020, https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions

563 Ibid., p. 90. For instance, bans have been passed at the city level in: San Francisco (California): San Francisco Administrative Code, Sec. 19b.2. Board of Supervisors Approval of Surveillance Technology Policy, https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-61746; Oakland (California): City of Oakland, Code of Ordinances, 9.64.045 - Prohibition on City's acquisition and/or use of Biometric Surveillance Technology and Predictive Policing Technology, https://library.municode.com/ca/oakland/codes/code_of_ordinances?nodeId=TIT9PUPEMOWE_CH9.64REACUSSUTE_9.64.045PRACUSBISUTEPRPOTE; Portland (Oregon): The City of Portland, Council Ordinance, 190113 Prohibit the acquisition and use of Face Recognition Technologies by City bureaus ordinance, 2020, https://efiles.portlandoregon.gov/Record/139452; and Minneapolis (Minnesota): Minneapolis Code of Ordinances, Title 2, Chapter 41, Article II. - Facial Recognition Technology, https://library.municode.com/mn/minneapolis/codes/code_of_ordinances?nodeId=COOR_TIT2AD_CH41INGO_ARTIIFARETE

564 A. Kak, "Regulating Biometrics: Global Approaches and Open Questions", AI Now Institute, September 1, 2020, https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions, pp. 91-92.

565 AP News, "Virginia lawmakers ban police use of facial recognition", March 29, 2021, https://apnews.com/article/technology-legislature-police-law-enforcement-agencies-legislation-033d77787d4e28559f08e5e31a5cb8f7

566 X. Landen, "Attorney general's office asks lawmakers to loosen ban on facial recognition", VTDigger, February 25, 2021, https://vtdigger.org/2021/02/25/attorney-generals-office-asks-lawmakers-to-loosen-ban-on-facial-recognition/

567 The Editorial Board of Los Angeles Daily News, "Opinion: Calif. Should Extend Facial Recognition Ban", Government Technology, April 6, 2022, https://www.govtech.com/policy/opinion-calif-should-extend-facial-recognition-ban; G. Lee, "California bill would regulate police use of facial recognition technology in body cams", KTVU Fox 2, March 9, 2023, https://www.fox2detroit.com/news/california-bill-would-regulate-police-use-of-facial-recognition-technology-in-body-cams; CBS San Franciscso, "Bill proposed to regulate facial recognition technology in policing", March 8, 2023, https://www.cbsnews.com/sanfrancisco/news/bill-proposed-to-regulate-facial-recognition-technology-in-policing/; C. Micheli, "Facial Recognition Legislation in California", California Globe, March 4, 2023, https://californiaglobe.com/articles/facial-recognition-legislation-in-california/

568 K. Kaye, "Police can use facial recognition again after ban in New Orleans, home to sprawling surveillance", Protocol, July 26, 2022, https://www.protocol.com/enterprise/new-orleans-surveillance-facial-recognition

569 R. Metz, "First, they banned facial recognition. Now they're not so sure", CNN Business, August 5, 2022, https://edition.cnn.com/2022/08/05/tech/facial-recognition-bans-reversed/index.html; J. Parker, "U.S. States and Cities Rethinking Bans, Setting Rules for Law Enforcement Use of Facial Recognition", Security Industry Association, May 10, 2022, https://www.securityindustry.org/2022/05/10/u-s-states-and-cities-rethinking-bans-setting-rules-for-law-enforcement-use-of-facial-recognition/

570 P. Dave, "U.S. cities are backing off banning facial recognition as crime rises", Reuters, May 12, 2022, https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/

571 BIPA regulates different types of biometrics. According to the BIPA definition, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Text of BIPA is available here: Illinois General Assembly, Public Act 095-0994, https://www.ilga.gov/legislation/publicacts/95/095-0994.htm

572 Capture or Use of Biometric Identifiers Act or CUBI for short, also known as Texas Business & Commerce Code 503.001, text available here: Texas State Legislature, Texas Business & Commerce Code 503.001, 2009, https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

573 J. Goldwater, M. Smigielski, K. Nelson, "State Biometric Legislation Developments", Lewis Brisbois Bisgaard & Smith LLP, August 18, 2021, https://lewisbrisbois.com/newsroom/legal-alerts/state-biometric-legislation-developments

574 J. Lewis, W. Crumpler, "Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape", Center for Strategic and International Studies, September 29, 2021, https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape

575 C. W. Savage, "Washington Enacts First-in-the-Nation State Law Regulating Governmental Use of Facial Recognition Technology", Davis Wright Tremaine, April 9, 2020, https://www.dwt.com/blogs/privacy--security-law-blog/2020/04/washington-state-facial-recognition-tech-law

576 Y. Luo, R. Guo, "Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead", 25 U. Pa. J.L. & Soc. Change 153, 2021, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1269&context=jlasc, p. 173

577 Washington State Legislature, SB 6280 - 2019-20, 2020, https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false#documentSection

578 E. Lostri, "Washington's New Facial Recognition Law", Center for Strategic and International Studies, April 3, 2020, https://www.csis.org/blogs/strategic-technologies-blog/washingtons-new-facial-recognition-law

579 A. Berengaut, "Washington State Passes Bill Limiting Government Use of Facial Recognition", Covington Inside Privacy, March 23, 2020, https://www.insideprivacy.com/united-states/state-legislatures/washington-state-passes-bill-limiting-government-use-of-facial-recognition/

580 J. Lee, "We Need a Face Surveillance Moratorium, Not Weak Regulations: Concerns about SB 6280", ACLU of Washington, March 31, 2020, https://www.aclu-wa.org/story/we-need-face-surveillance-moratori-

um-not-weak-regulations-concerns-about-sb-6280; E. Lostri, "Washington's New Facial Recognition Law",Center for Strategic and International Studies, April 3, 2020, https://www.csis.org/blogs/strategic-technologies-blog/washingtons-new-facial-recognition-law

581 P. Dave, J. Dastin, "Washington State signs facial recognition curbs into law; critics want ban", Reuters, March 31, 2020, https://www.reuters.com/article/us-washington-tech-idUSKBN21I3AS; D. Gershgorn, "A Microsoft Employee Literally Wrote Washington's Facial Recognition Law", OneZero, April 3, 2020, https://onezero.medium.com/a-microsoft-employee-literally-wrote-washingtons-facial-recognition-legislation-aab950396927; B. Smith, "Finally, progress on regulating facial recognition", Microsoft, March 31, 2020, https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/

582 One summary is available here: A. Berengaut, "Washington State Passes Bill Limiting Government Use of Facial Recognition", Covington Inside Privacy, March 23, 2020, https://www.insideprivacy.com/united-states/state-legislatures/washington-state-passes-bill-limiting-government-use-of-facial-recognition/

583 Text of the law with the summary is available here: Colorado General Assembly, SB22-113, Artificial Intelligence Facial Recognition, 2022, https://leg.colorado.gov/bills/sb22-113; Legislative timeline is available here: Digital Policy Alert, "United States of America: Colorado: Law on facial recognition technology (Senate Bill 22-113)", https://digitalpolicyalert.org/change/2828-colorado-law-on-facial-recognition-technology-senate-bill-22-113

584 L. Foster Freedman, "Colorado Law Restricts Use of Facial Recognition Technology by Government Agencies", Robinson+Cole , June 15, 2022, https://www.dataprivacyandsecurityinsider.com/2022/06/colorado-law-restricts-use-of-facial-recognition-technology-by-government-agencies/; H. Metzger, "Task force to assess use of facial recognition by Colorado law enforcement, government", Colorado Politics, June 9, 2022, https://www.coloradopolitics.com/legislature/task-force-to-assess-use-of-facial-recognition-by-colorado-law-enforcement-government/article_52846144-e83e-11ec-b930-7fe52b4e1214.html

585 General Assembly of Virginia, Code of Virginia, § 15.2-1723.2., 2021, https://law.lis.virginia.gov/vacode/title15.2/chapter17/section15.2-1723.2/; General Assembly of Virginia, Code of Virginia, § 23.1-815.1, 2021, https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2031ER+hil

586 B. Atkinson, "Virginia Bill to Put De Facto Ban on Facial Recognition Tech", Government Technology, April 8, 2021, https://www.govtech.com/policy/virginia-bill-to-put-de-facto-ban-on-facial-recognition-tech.html; Robinson & Cole LLP, "Virginia Law Bans Local Police Use of Facial Recognition Technology", The National Law Review, April 22, 2021, https://www.natlawreview.com/article/virginia-law-bans-local-police-use-facial-recognition-technology

587 The detailed legislative history can be found here: A. Powers, K. Simon, J. Spivack, "From Ban to Approval: What Virginia's Facial Recognition Technology Law Gets Wrong", 26 Rich. Pub. Int. L. Rev. 155, 2023, https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1553&context=pilr

588 S. C. Weston, "Can Police in Virginia Use Facial Recognition if They Suspect Criminal Activity?", November 16, 2022, https://scwestonlaw.com/can-police-in-virginia-use-facial-recognition-if-they-suspect-criminal-activity/

589 A. McGibbon, "Police use of facial recognition tech resumes with guardrails", VPM, March 3, 2023, https://www.vpm.org/news/2023-03-03/virginia-facial-recognition-law-enforcement-privacy; ACLU of Virginia, "ACLU-VA's Statement on Gov. Youngkin's Actions on Facial Recognition Technology", April 14, 2022, https://www.acluva.org/en/press-releases/aclu-vas-statement-gov-youngkins-actions-facial-recognition-technology

590 Text of the law is available here: General Assembly of Virginia, SB 741 Facial recognition technology; authorised uses, 2022, https://lis.virginia.gov/cgi-bin/legp604.exe?221+sum+SB741

591 Text of the model policy is available here: Commonwealth of Virginia, "State Police Model Facial Recognition Technology Policy", December 31, 2022, https://vsp.virginia.gov/wp-content/uploads/2023/01/State-Police-Model-Facial-Recognition-Technology-Policy.doc

592 Text of the law is available here: Maine State Legislature, 25 Maine Revised Statutes § 6001. Facial surveillance, 2021, https://legislature.maine.gov/statutes/25/title25sec6001.html

593 ACLU of Maine, "Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country", June 30, 2021, https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country; A. Beyea, M. Kebede, "Maine's facial recognition law shows bipartisan support for protecting privacy", TechCrunch, July 20, 2021, https://techcrunch.com/2021/07/20/maines-facial-recognition-law-shows-bipartisan-support-for-protecting-privacy/; J. Bryant, "Maine passes statewide facial recognition ban", IAPP, July 1, 2021, https://iapp.org/news/a/maine-passes-statewide-facial-recognition-ban/; D. Gershgorn, "Maine passes the strongest state facial recognition ban yet", The Verge, June 30, 2021, https://www.theverge.com/2021/6/30/22557516/maine-facial-recognition-ban-state-law; I. Bonifacic, "Maine bans facial recognition technology from schools and most police work", Engadget, June 30, 2021, https://www.engadget.com/maine-facial-recognition-law-191252742.html; S. Ikeda, "Maine Becomes First State To Pass Broad Government Ban on Facial Recognition Technology", CPO Magazine, July 8, 2021, https://www.cpomagazine.com/data-privacy/maine-becomes-first-state-to-pass-broad-government-ban-on-facial-recognition-technology/

594 Statewatch, "EU: Got a driving licence? You're going in a police line-up", February 21, 2022, https://www.statewatch.org/news/2022/february/eu-got-a-driving-licence-you-re-going-in-a-police-line-up/

595 Text of the law: Utah State Legislature, S.B. 34 Governmental Use of Facial Recognition Technology, 2021, https://le.utah.gov/~2021/bills/static/SB0034.html

596 FindBiometrics, "Utah State Legislature Passes Facial Recognition Bill", March 5, 2021, https://findbiometrics.com/utah-state-legislature-passes-facial-recognition-bill-030504/; FindBiometrics, "Utah Agency Adopts Internal Guidelines In Lieu of State Facial Recognition Law", October 6, 2020, https://findbiometrics.com/utah-agency-adopts-internal-guidelines-lieu-state-facial-recognition-law-100606/; FindBiometrics, "Utah Poll Finds Public Support for Facial Recognition", February 13, 2020, https://findbiometrics.com/biometrics-news-utah-poll-finds-public-support-facial-recognition-021308/;Results of the poll in question are available here: Suffolk University, Salt Lake Tribune, Utah Poll, January 2020, https://www.suffolk.edu/-/media/suffolk/documents/academics/research-at-suffolk/suprc/polls/other-states/2020/2_18_2020_

marginals_pdftxt.pdf?la=en&hash=440698A3312913CAF76630A78BD-07E142631D34B

597 Text of the legislation is available here: Massachusetts General Court, General Laws, Part I, Title II, Chapter 6, Section 220: Facial recognition searches, 2020, https://malegislature.gov/Laws/GeneralLaws/PartI/TitleII/Chapter6/Section220; There is also a law in Massachusetts that regulates FRT use by private entities: Massachusetts General Court, Bill H.117, An Act to provide facial recognition accountability and comprehensive enforcement, 2021, https://malegislature.gov/Bills/192/H117

598 S. Solis, "Compromise police reform bill heads to Massachusetts Gov. Charlie Baker's desk", MassLive, December 23, 2020, https://www.masslive.com/politics/2020/12/compromise-police-reform-bill-heads-to-massachusetts-gov-charlie-bakers-desk.html

599 The law does contain a definition of "other remote biometric recognition" that includes gait and voice, but does not regulate the use of the technology for such remote recognition. It relies on such a definition to clarify the situations in which facial recognition tools can be used. See also: ACLU of Massachusetts, "Limited face recognition regulations take effect today", July 1, 2021, https://www.aclum.org/en/news/limited-face-recognition-regulations-take-effect-today; E. Peaslee, "Massachusetts Pioneers Rules For Police Use Of Facial Recognition Tech", NPR, May 7, 2021, https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech; J. Cote, "Facial recognition: What to know about the Massachusetts police reform bill's restrictions on the controversial tech", MassLive, December 6, 2020, https://www.masslive.com/police-fire/2020/12/facial-recognition-what-to-know-about-the-massachusetts-police-reform-bills-restrictions-on-the-controversial-tech.html

600 K. Hill, "How One State Managed to Actually Write Rules on Facial Recognition", The New York Times, February 27, 2021, https://www.nytimes.com/2021/02/27/technology/Massachusetts-facial-recognition-rules.html

601 ACLU of Massachusetts, "Limited face recognition regulations take effect today", July 1, 2021, https://www.aclum.org/en/news/limited-face-recognition-regulations-take-effect-today

602 ACLU of Massachusetts, "Press Pause on Face Surveillance", June 2023, https://www.aclum.org/en/campaigns/press-pause-face-surveillance

603 Facial Recognition Commission of Massachusetts, https://frcommissionma.com/

604 Section 105, 253 of the Acts of 2020, available here: Massachusetts General Court, Session Laws, Chapter 253, An Act Relative To Justice, Equity And Accountability In Law Enforcement In The Commonwealth, https://malegislature.gov/Laws/SessionLaws/Acts/2020/Chapter253

605 J. Nash, "Massachusetts panel says use of facial recognition should be restricted to state police", Biometric Update, Mar 24, 2022, https://www.biometricupdate.com/202203/massachusetts-panel-says-use-of-facial-recognition-should-be-restricted-to-state-police; W. Katcher, "Massachusetts Facial Recognition Commission issues recommendations on use of controversial technology", MassLive, March 22, 2022, https://www.masslive.com/news/2022/03/massachusetts-facial-recognition-commission-issues-recommendations-on-use-of-controversial-technology.html; S. Schoenberg,

"Commission calls for limiting police use of facial recognition technology", CommonWealth Magazine, March 22, 2022, https://commonwealthmagazine.org/criminal-justice/commission-calls-for-limiting-police-use-of-facial-recognition-technology/; J. Bonilla, "Should facial recognition be used in Massachusetts? New report says to limit use", wickedlocal.com, June 29, 2022, https://www.wickedlocal.com/story/regional/massachusetts/2022/06/29/facial-recognition-use-commission-suggests-documenting-limiting-massachusetts-aclu-digital-fourth/9660776002/

606 Text of the law is available here: Alabama Legislature, AL SB56, 2022, https://legiscan.com/AL/bill/SB56/2022

607 Text as proposed: Alabama Legislature, AL SB56, Introduced 2022, https://legiscan.com/AL/text/SB56/id/2470282

608 A facial recognition service was defined as software, an algorithm, a product, or an application that collects or electronically analyses information for the purpose of identifying an individual by using technology capable of uniquely identifying or verifying a person by comparing and analysing patterns based on that individual's facial contours.

609 M. Maharrey, "Alabama Senate Passes Bill to Limit Warrantless Use of Facial Recognition", Tenth Amendment Center, February 2, 2022, https://blog.tenthamendmentcenter.com/2022/02/alabama-senate-passes-bill-to-limit-warrantless-use-of-facial-recognition/; B. Moseley, "Senate passes bill restricting the use of facial recognition technology by law enforcement", 1819 News, February 2, 2022, https://1819news.com/news/item/senate-passes-bill-restricting-the-use-of-facial-recognition-technology-by-law-en-02-02-2022

610 J. Parker, "U.S. States and Cities Rethinking Bans, Setting Rules for Law Enforcement Use of Facial Recognition", Security Industry Association, May 10, 2022, https://www.securityindustry.org/2022/05/10/u-s-states-and-cities-rethinking-bans-setting-rules-for-law-enforcement-use-of-facial-recognition/

611 D. Pillion, "Alabama police using facial recognition to ID Capitol riot suspects", AL.com, January 9, 2021, https://www.al.com/news/2021/01/alabama-police-using-facial-recognition-to-id-capitol-riot-suspects.html; A. Ramey, "Investigating Alabama's use of facial recognition technology", NBC 15 News, February 26, 2021, https://mynbc15.com/news/local/investigating-alabamas-use-of-facial-recognition-technology

612 Text of the law is available here: Vermont General Assembly, Act No. 166 (S.124), 2020, https://legislature.vermont.gov/bill/status/2020/S.124

613 There is an exception with respect to law enforcement use of drones, under the special legislation that regulates drones use.

614 X. Landen, "Attorney general's office asks lawmakers to loosen ban on facial recognition", VTDigger, February 25, 2021, https://vtdigger.org/2021/02/25/attorney-generals-office-asks-lawmakers-to-loosen-ban-on-facial-recognition/; J. Parker, "Most State Legislatures Have Rejected Bans and Severe Restrictions on Facial Recognition", Security Industry Association, July 9, 2021, https://www.securityindustry.org/2021/07/09/most-state-legislatures-have-rejected-bans-and-severe-restrictions-on-facial-recognition/

615 Text of the law is available here: Vermont General Assembly, Act No. 17 (H.195), 2021, https://legislature.vermont.gov/bill/status/2022/H.195

616 Vermont Criminal Justice Council, "Facial Recognition Technology Working

Group", https://vcjc.vermont.gov/council/committees/facial-recognition-technology-working-group

617 Text of the law is available here: Kentucky General Assembly, Senate Bill 176, 2022, https://apps.legislature.ky.gov/record/22rs/sb176.html

618 J. Parker, "U.S. States and Cities Rethinking Bans, Setting Rules for Law Enforcement Use of Facial Recognition", Security Industry Association, May 10, 2022, https://www.securityindustry.org/2022/05/10/u-s-states-and-cities-rethinking-bans-setting-rules-for-law-enforcement-use-of-facial-recognition/

619 AIAAIC, "Robert Williams facial recognition wrongful arrest", April 2021 , https://www.aiaaic.org/aiaaic-repository/ai-and-algorithmic-incidents-and-controversies/robert-williams-facial-recognition-wrongful-arrest; T. Ryan-Mosley, "The new lawsuit that shows facial recognition is officially a civil rights issue", MIT Technology Review, April 14, 2021, https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/

620 E. Anderson, "Controversial Detroit facial recognition got him arrested for a crime he didn't commit", Detroit Free Press, July 10, 2020, https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/

621 R. Darin Goldberg, "You Can See My Face, Why Can't I? Facial Recognition and Brady", Columbia Human Rights Law Review, April 12, 2021, https://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-and-brady/#post-1679-footnote-ref-19

622 ACLU of Massachusetts, "ACLU v. Department of Justice", 2019, https://www.aclum.org/en/cases/aclu-v-department-justic

623 R. Mac, K. Hill, "Clearview AI settles suit and agrees to limit sales of facial recognition database.", The New York Times, May 9, 2022, https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html; R. Metz, "Clearview AI agrees to restrict US sales of facial recognition mostly to law enforcement", CNN Business, May 9, 2022, https://edition.cnn.com/2022/05/09/tech/clearview-ai-aclu-settlement/index.html; ACLU of Illinois, "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law", May 9, 2022, https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

624 H. Tsukayama, "Trends in biometric information regulation in the USA", Ada Lovelace Institute, July 5, 2022, https://www.adalovelaceinstitute.org/blog/biometrics-regulation-usa/; E. Barlow Keener, "Facial Recognition: A New Trend in State Regulation", American Bar Association, April 25, 2022, https://www.americanbar.org/groups/business_law/publications/blt/2022/05/facial-recognition/; Some cases were not successful: R. Westhead, "Blackhawks resolve lawsuit over alleged use of facial recognition software", TSN, September 1, 2021, https://www.tsn.ca/rick-westhead-chicago-blackhawks-illegally-used-facial-recognition-software-on-fans-lawsuit-says-1.1688479; FindBiometrics, "Plaintiff Abandons BIPA Lawsuit Against Chicago Blackhawks", September 8, 2021, https://findbiometrics.com/plaintiff-abandons-bipa-lawsuit-against-chicago-blackhawks-090807/

625 P. McKnight, "Historic Biometric Privacy Suit Settles for $650 Million", Business Law Today from ABA, January 28, 2021, https://businesslawtoday.org/2021/01/historic-biometric-privacy-suit-settles-650-million/; J. Bryant,

"Facebook's $650M BIPA settlement 'a make-or-break moment'", IAPP, March 5, 2021, https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/

626 F. M. Trujillo, J. Frankel, "Texas Starts Enforcing its Biometric Law", ZwillGen Blog, February 18, 2022, https://www.zwillgen.com/privacy/texas-cubi-law-and-biometric-privacy; D. Bartz, "Texas sues Meta's Facebook over facial-recognition practices", Reuters, February 14, 2022, https://www.reuters.com/technology/texas-sues-meta-over-facebooks-facial-recognition-practices-report-2022-02-14/

627 Hunton Privacy Blog, "Judge Approves $92 Million TikTok Settlement", August 9, 2022, https://www.huntonprivacyblog.com/2022/08/09/judge-approves-92-million-tiktok-settlement/; N. Sakin, "TikTok settlement highlights power of privacy class actions to shape US protections", IAPP, Mar 23, 2021, https://iapp.org/news/a/tiktok-settlement-highlights-power-of-privacy-class-actions-to-shape-u-s-protections/

628 A. Malik, "Snap agrees to $35 million settlement in Illinois privacy lawsuit", TechCrunch, August 24, 2022, https://techcrunch.com/2022/08/24/snap-35-million-settlement-in-illinois-bipa/; Top Class Actions, "Snapchat biometric privacy $35M class action settlement", November 1, 2022, https://topclassactions.com/lawsuit-settlements/closed-settlements/snapchat-biometric-privacy-35m-class-action-settlement/

629 K. Hurler, "Google Settles in $100 Million Illinois Photo Privacy Lawsuit", Gizmodo, June 14, 2023, https://gizmodo.com/with-a-new-developer-framework-building-in-xr-is-easie-1850491958; NBC Chicago, "Everything To Know About Google Class-Action Settlement For Illinois Residents", October 1, 2022, https://www.nbcchicago.com/news/local/everything-to-know-about-google-class-action-settlement-for-illinois-residents/2955833/

630 H. Swart, A. Munoriyarwa, "Video Surveillance in Southern Africa: Case studies of security camera systems in the region", Media Policy and Democracy Project, May 2020, https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/video_surveillance_in_southern_africa_-_security_camera_systems_in_the_region.pdf

631 Global Voices, "How Zimbabwe is building a Big Brother surveillance state", January 10, 2023, https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/

632 Ibid.

633 F. Mutsaka, "Zimbabwe's imposing new Chinese-funded parliament opens-Mutsaka", AP News, November 23, 2022, https://apnews.com/article/africa-china-asia-zimbabwe-d7176d0e7ed5997e50c89d226a34d2e9

634 Privacy International, "Huawei and Surveillance in Zimbabwe", November 18, 2021, https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe

635 MISA Zimbabwe, "Digest: Facial recognition technology and privacy rights", May 29, 2018, https://zimbabwe.misa.org/2018/05/29/digest-facial-recognition-technology-privacy-rights/; See also:

A. Hawkins, "Beijing's Big Brother Tech Needs African Faces", Foreign Policy, July 24, 2018,https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/

636 K. Muleya, "African dream of 'smart cities' remains strong", Warp News, October 16, 2021, https://www.warpnews.org/human-progress/african-dream-of-smart-cities-remains-strong/

637 The Standard, "Creating a surveillance state: ED govt zooms in for critics with Chinese help", March 1, 2020, https://thestandard.newsday.co.zw/2020/03/01/creating-surveillance-state-ed-govt-zooms-critics-chinese-help

638 Ibid., See also: Privacy International, "Huawei and Surveillance in Zimbabwe", November 18, 2021, https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe

639 P. Masau, "Face of the Future", ChinAfrica, August 13, 2018, http://www.chinafrica.cn/Homepage/201808/t20180813_800138079.html

640 Privacy International, "Huawei and Surveillance in Zimbabwe", November 18, 2021, https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwel; Africa Defense Forum, "Zimbabwe Turns to Chinese Technology to Expand Surveillance of Citizens", January 17, 2023, https://adf-magazine.com/2023/01/zimbabwe-turns-to-chinese-technology-to-expand-surveillance-of-citizens/

641 Global Voices, "How Zimbabwe is building a Big Brother surveillance state", January 10, 2023, https://globalvoices.org/2023/01/10/how-zimbabwe-is-building-a-big-brother-surveillance-state/

642 A. Macdonald, "Zimbabwe govt faces criticism over biometric surveillance project for new smart city", Biometric Update, February 28, 2023, https://www.biometricupdate.com/202302/zimbabwe-govt-faces-criticism-over-biometric-surveillance-project-for-new-smart-city

643 F. S. Matiashe, "Zimbabwe's cyber city: Urban utopia or surveillance menace?", Context, February 21, 2023, https://www.context.news/surveillance/zimbabwes-cyber-city-urban-utopia-or-surveillance-menace

644 DataGuidance, "Zimbabwe - Summary", https://www.dataguidance.com/jurisdiction/zimbabwe

645 MISA Zimbabwe, "Analysis of the Data Protection Act", December 6, 2021, https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/

646 Ibid.

647 T. Kachiko, "Data Protection Bill criticised", NewsDay Zimbabwe, December 17, 2021,https://www.newsday.co.zw/2021/12/data-protection-bill-criticised ; See also: K. Chimhangwa, "Weaponising the law: Zimbabwe's new frontier in digital rights repression", Global Voices, April 26, 2022, https://globalvoices.org/2022/04/26/weaponising-the-law-zimbabwes-new-frontier-in-digital-rights-repression/

648 K. Chimhangwa, "Weaponising the law: Zimbabwe's new frontier in digital rights repression", Global Voices, April 26, 2022, https://globalvoices.org/2022/04/26/weaponising-the-law-zimbabwes-new-frontier-in-digital-rights-repression/

649 C. S. Mavhunga, D. McKenzie, "Social media access restored in Zimbabwe by court order", CNN, January 23, 2019, https://edition.cnn.com/2019/01/21/africa/zimbabwe-protests-internet-shutdown-ruling-intl/index.html

650 Veritas, "Court Watch 1/2019 - The Internet Shutdown: The High Court's Ruling of 21st January", January 30, 2019, https://www.veritaszim.net/node/3397

651 F. Mudzingwa, "[Breaking] High Court Declares That Internet Blockade Was Illegal And Social Media Access Must Be Restored", Techzim, January 21, 2019, https://www.techzim.co.zw/2019/01/breaking-high-court-declares-that-internet-blockade-was-illegal/

652 Veritas, "Court Watch 1/2019 - The Internet Shutdown: The High Court's Ruling of 21st January", January 30, 2019, https://www.veritaszim.net/node/3397

653 M. Dzirutwe, "Zimbabwe court says internet shutdown illegal as more civilians detained", Reuters, January 21, 2019, https://www.reuters.com/article/us-zimbabwe-politics-idUSKCN1PF11M

654 P. Königs, "Government Surveillance, Privacy, and Legitimacy", Philosophy and Technology 35(8), 2022, https://doi.org/10.1007/s13347-022-00503-9

655 Council of Europe, "Thematic Factsheet: Mass Surveillance", July 2018, https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e

656 Garante per la Protezione dei Dati Personali, "Facial recognition: the SARI Real Time system is not compliant with privacy laws", April 16, 2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575842#english

657 E. Jakubowska, "Remote biometric identification: a technical & legal guide", EDRi, January 23, 2023, https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/

658 European Parliament, "Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters", July 17, 2021, https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

659 Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach", November 25, 2022, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf

660 Hindustan Times, "'Only 2 percent accuracy' in Delhi police facial recognition software: High Court told", August 23, 2018, https://www.hindustantimes.com/cities/only-2-percent-accuracy-in-delhi-police-facial-recognition-software-high-court-told/story-D4d2oP3PAVn8OwyCqpA4FO.html

661 P. Fussey, A. Sandhu, "Surveillance arbitration in the era of digital policing", Theoretical Criminology 26(1), 3-22, 2022, https://doi.org/10.1177/1362480620967020

662 La Quadrature du Net, "La Reconnaissance Faciale Des Manifestant□es Est Déjà Autorisée", November 18, 2019, https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/

663 N. A. Smuha, "Beyond the Individual: Governing AI's Societal Harm", Internet Policy Review 10(3), 2021, https://doi.org/10.14763/2021.3.1574

664 Ibid., p. 5

665 K. Hao, "This is How We Lost Control of Our Faces", MIT Technology Review, February 5, 2021, https://www.technologyreview.com/2021/02/05/1017388/ai-deep-learning-facial-recognition-data-history/; P. Guest, "Singapore's Tech-Utopia Dream is Turning Into a Surveillance State Nightmare", Rest of World, November 16, 2021, https://restofworld.org/2021/singapores-tech-utopia-dream-is-turning-into-a-surveillance-state-nightmare/; V. Dodd, "UK police use of live facial recognition unlawful and unethical, report finds", The Guardian, October 27, 2022, https://www.theguardian.com/technology/2022/oct/27/live-facial-recognition-police-study-uk; European Digital Rights (EDRi), "Ban biometric Mass Surveillance", 2020, https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

666 H. Boghosian, "How Fear of Government Surveillance Influences Our Behavior", Literary Hub, July 15, 2021, https://lithub.com/how-fear-of-government-surveillance-influences-our-behavior/

667 A. Najibi, "Racial Discrimination in Face Recognition Technology", Harvard University, October 24, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

668 S. Perkowitz, "The Bias in the Machine: Facial Recognition Technology and Racial Disparities", MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2021 (February), https://doi.org/10.21428/2c646de5.62272586.

669 European Digital Rights (EDRi), "Beyond Debiasing: Regulating AI and Its Inequalities", 2021 https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf

670 Ibid., p. 10

671 H. Suresh, J. Guttag, "A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle", Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '21), Association for Computing Machinery, Article 17, 1-9, 2021, https://doi.org/10.1145/3465416.3483305

672 V. Joler, M. Pasquinelli, "The Nooscope Manifested: AI as Instrument of Knowledge Extractivism", 2020, https://nooscope.ai/

673 D. Leslie, "Understanding the Bias in Facial Recognition Technology: An Explainer", The Alan Turing Institute, 2020, https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf

674 T. Bolukbasi et al., "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", NIPS'16: Proceedings of the 30th International Conference on Neural Information Processing Systems, 4356–4364, December 2016, https://dl.acm.org/doi/pdf/10.5555/3157382.3157584

675 M. Ngan, P. Grother, "Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms, NIST Interagency Report 8052", National Institute of Standards and Technology, April 2015, https://doi.org/10.6028/NIST.IR.8052

676 J. Buolamwini, T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Conference on Fairness, Accountability and Transparency, Proceedings of Machine Learning Research 81:1–15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

677 J. Buolamwini et al., "Gender Shades", Algorithmic Justice League, 2018, http://gendershades.org/overview.html

678 J. Angwin et al., "Machine Bias", ProPublica, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

679 A. Nellis, "The Color of Justice: Racial and Ethnic Disparity in State Prisons", The Sentencing Project, October 13, 2021, https://www.sentencingproject.org/reports/the-color-of-justice-racial-and-ethnic-disparity-in-state-prisons-the-sentencing-project/

680 H. Suresh, J. Guttag, "A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle", op. cit., p. 5

681 A. Sandhu, P. Fussey, "The 'uberization of policing'? How police negotiate and operationalise predictive policing technology", Policing and Society 31 (1), 66-81, 2021, https://doi.org/10.1080/10439463.2020.1803315, p. 76

682 H. Suresh, J. Guttag, "A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle", op. cit., p. 5

683 T. Blevins et al., "Automatically Processing Tweets from Gang-Involved Youth: Towards Detecting Loss and Aggression", Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: Technical Papers, 2196–2206, December 2016, https://aclanthology.org/C16-1207.pdf

684 G. Mauro, H. Schellmann, "'There is no standard': investigation finds AI algorithms objectify women's bodies", The Guardian, February 8, 2023, https://www.theguardian.com/technology/2023/feb/08/biased-ai-algorithms-racy-women-bodies

685 Ibid.

686 I. D. Raji et al., "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing", AIES '20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 145–151, February 2020, https://doi.org/10.1145/3375627.3375820

687 Pete Fussey, @PeteFussey, "1. This is a technical evaluation. Doesn't examine policing uses. While has merit, does not follow that the findings (a) can be generalised (b) legitimate entire FRT use or (c) even fully address issues of bias 2/15", Twitter, April 5, 2023, https://twitter.com/PeteFussey/status/1643721120971993090

688 L. Zedner, "Security", Routledge, 2009, p. 2

689 C. Whelan, "Surveillance, security and sporting mega events: Toward a research agenda on the organisation of security networks", Surveillance and Society 11(4): Surveillance and Sport, 392-404, 2014, http://dx.doi.org/10.24908/ss.v11i4.4722, p. 395

690 C. Reilly, "Facial-recognition software inaccurate in 98% of cases, report finds", CNET, May 13, 2018, https://www.cnet.com/tech/tech-industry/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/

691 G. Pisanu et al., "Surveillance Tech in Latin America: Made Abroad, Deployed at Home", Access Now, August 9, 2021, https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/

692 E. Hinz, "How Myanmar's junta uses Chinese surveillance technology",

Deutsche Welle, July 28, 2022, https://www.dw.com/en/how-myanmars-junta-is-using-chinese-facial-recognition-technology/a-62624413

693 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Track and target: FAQ on Myanmar CCTV cameras and facial recognition", Access Now, August 4, 2022, https://www.accessnow.org/myanmar-cctv-cameras/

694 Access Now, "Resist Myanmar's digital coup: stop the military consolidating digital control", February 8, 2022, https://www.accessnow.org/press-release/myanmars-digital-coup-statement/

695 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Track and target: FAQ on Myanmar CCTV cameras and facial recognition", Access Now, August 4, 2022, https://www.accessnow.org/myanmar-cctv-cameras/

696 Ibid.

697 M. Clark, "Leaked documents link Huawei to China's domestic spying in Xinjiang", The Verge, December 15, 2021, https://www.theverge.com/2021/12/14/22834860/huawei-leaked-documents-xinjiang-region-uyghur-facial-recognition-prisons-surveillance

698 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Track and target: FAQ on Myanmar CCTV cameras and facial recognition", Access Now, August 4, 2022, https://www.accessnow.org/myanmar-cctv-cameras/

699 M. Maung, "Myanmar's Prisoner Release Still Leaves Thousands Detained", Human Rights Watch, May 6, 2023, https://www.hrw.org/news/2023/05/06/myanmars-prisoner-release-still-leaves-thousands-detained

700 Assistance Association for Political Prisoners Burma (AAPPB) is a human rights organisation advocating for the release of political prisoners in Burma and for the improvement of their quality of life during and after incarceration: Assistance Association for Political Prisoners Burma, "Home", https://aappb.org/

701 E. Hinz, "How Myanmar's junta uses Chinese surveillance technology", Deutsche Welle, July 28, 2022, https://www.dw.com/en/how-myanmars-junta-is-using-chinese-facial-recognition-technology/a-62624413

702 Amnesty International, "Myanmar: Detainees tortured to crush opposition to coup", August 2, 2022, https://www.amnesty.org/en/latest/news/2022/08/myanmar-detainees-tortured-to-crush-opposition-to-coup/

703 Free Expression Myanmar, "Myanmar's new Electronic Transactions Law Amendment", February 18, 2021, https://freeexpressionmyanmar.org/myanmars-new-electronic-transactions-law-amendment/

704 G. Benjamin, D. Sivaprakasam, W. P. Myint, "Myanmar IMEI FAQ: how the junta could disconnect the resistance", Access Now, July 7, 2022, https://www.accessnow.org/myanmar-imei/

705 UN Human Rights Office, "The international community's response to the crisis in Myanmar is failing, and that failure has contributed to a lethal downward spiral that is devastating the lives of millions of people", Tom Andrews, UN Special Rapporteur on the human rights situation in Myanmar ("UN expert urges Japan to step up pressure on Myanmar junta", Press release, 28 April 2023); OHCHR, "UN expert urges Japan to step up pressure on Myanmar junta", April 28, 2023, https://www.ohchr.org/en/press-releases/2023/04/un-expert-urges-japan-step-pressure-myanmar-junta

706 Wolfgang Merkel's classification of political systems: democracies (embedded and defective) and autocracies (authoritarianism and totalitarianism); W. Merkel, "Embedded and defective democracies", Democratisation 11:5, 33-58, 2004

707 S. A. Cole, "Imprint of the Raj: How Fingerprinting was Born in Colonial India (review)", Technology and Culture 46(1), 252-253, 2005, Project MUSE, https://doi.org/10.1353/tech.2005.0010

708 B. W. Goossen, "Measuring Mennonitism: Racial Categorization in Nazi Germany and Beyond", Journal of Mennonite Studies, Vol. 34, 2016, https://jms.uwinnipeg.ca/index.php/jms/article/view/1651

709 Y. Gorokhovskaia, A. Shahbaz, A. Slipowitz, "Marking 50 Years in the Struggle for Democracy", Freedom House, March 2023, https://freedomhouse.org/report/freedom-world/2023/marking-50-years

710 Human Rights Watch, "Myanmar: No Justice, No Freedom for Rohingya 5 Years On", August 24, 2022, https://www.hrw.org/news/2022/08/24/myanmar-no-justice-no-freedom-rohingya-5-years

711 Ministry of Interior of Serbia, "Impact Assessment on Data Protection Through the Use of Contemporary Surveillance Technologies", September 2019, https://www.sharefoundation.info/wp-content/uploads/MUP-Procena-uticaja-obrade-na-zastitu-podataka-o-licnosti-koriscenjem-sistema-video-nadzora.pdf (in Serbian)

712 Commissioner for Information of Public Importance and Personal Data Protection of Serbia, "Opinion on the Ministry of Interior's Data Protection Impact Assessment for the Video Surveillance System", November 2019, https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739FD85A9B (in Serbian)

713 SHARE Conference, @SHAREConference, "Postavljanje Huawei kamera na Trgu Republike [Setting up Huawei cameras at Republic's Square]", Twitter, June 12, 2019, https://twitter.com/ShareConference/status/1138774544632680449

714 hiljadekamera Twitter account, @hiljadekamera, https://twitter.com/hiljadekamera

715 In official documents, the terms "Safe City" and "Safe Society" are used interchangeably by Huawei and the Ministry of Interior of Serbia.

716 D. Krivokapić, M. Bajić, B. Perkov, "Biometrics in Belgrade: Serbia's Path Shows Broader Dangers of Surveillance State", Heinrich Boell Stiftung, May 19, 2021, https://eu.boell.org/en/2021/05/19/biometrics-belgrade-serbias-path-shows-broader-dangers-surveillance-state

717 Huawei, "Huawei Safe City Solution: Safeguards Serbia", August 23, 2018, accessible at: https://archive.li/pZ9HO

718 Ministry of Interior of Serbia, "Impact Assessment on Data Protection Through the Use of Contemporary Surveillance Technologies Within the 'Safe Society' Project in Belgrade", March 2020, https://www.sharefoundation.info/wp-content/uploads/Procena_uticaja_2_0.pdf (in Serbian)

719 SHARE Foundation, "Total Surveillance Law Proposed in Serbia", September 21, 2021, https://www.sharefoundation.info/en/total-surveillance-law-proposed-in-serbia/

720 SHARE Foundation, "Comments on the Draft Law on Internal Affairs", September 2021, https://www.sharefoundation.info/wp-content/uploads/Draft-Law-on-Internal-Affairs_Comments_SHARE-Foundation.pdf

721 SHARE Foundation, "Draft Withdrawal a Step Towards Moratorium on Biometric Surveillance", September 23, 2021, https://www.sharefoundation.info/en/draft-withdrawal-a-step-towards-moratorium-on-biometric-surveillance/

722 Ministry of Interior of Serbia, "Draft Law on Internal Affairs", December 2022, http://www.mup.gov.rs/wps/wcm/connect/4ceb4620-bcb6-4370-b55a-8f9dbb6f558d/НАЦРТ+ЗАКОНА+О+УНУТРАШЊИМ+ПОСЛОВИМА.pdf?MOD=AJPERES&CVID=ojJiNDS (in Serbian)

723 Ministry of Interior of Serbia, "Draft Law on Data Processing and Records in Internal Affairs, December 2022, http://www.mup.gov.rs/wps/wcm/connect/7ecd0fe1-018d-4445-bf20-b00559bcb13f/Нацрт+закона+о+обради+података+и+евиденцијама+у+области+унутрашњих+послова.pdf?MOD=AJPERES&CVID=ojJjNSn (in Serbian)

724 Ministry of Interior of Serbia, "Assessment of the Impact of Personal Data Processing Using Biometric Data Processing Software in the Video Surveillance System of the Ministry of Interior [of the Republic of Serbia] on the Protection of Personal Data", [unofficial translation by SHARE Foundation for reference purposes], December 2022, https://www.sharefoundation.info/wp-content/uploads/Impact-Assessment_SHARE-translation_ENG.pdf

725 SHARE Foundation, "What Are the Provisions of New Policing Draft Laws", December 16, 2022, https://www.sharefoundation.info/en/new-policing-draft-laws/

726 The Government of the Republic of Serbia, "Draft Law on Internal Affairs Withdrawn From the Adoption Procedure", December 26, 2022, https://www.srbija.gov.rs/vest/en/199975/draft-law-on-internal-affairs-withdrawn-from-the-adoption-procedure.php

727 SHARE Foundation, "Round Two of the Battle Against Mass Biometric Surveillance", January 9, 2023, https://www.sharefoundation.info/en/round-two-of-the-battle-against-mass-biometric-surveillance/

728 Reclaim Your Face, "The problem", https://reclaimyourface.eu/the-problem/

729 K. Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", The New York Times, December 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

730 G. Ridgeway, "Analysis of Racial Disparities in the New York Police Department's Stop, Question, and Frisk Practices", RAND Corporation, 2007, https://www.rand.org/pubs/technical_reports/TR534.html

731 Office of the New York State Comptroller, Division of State Government Accountability, "Artificial Intelligence Governance: Report 2021-N-10", February 2023, https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21n10.pdf

732 Office of the New York State Comptroller, Division of State Government Accountability, "Artificial Intelligence Governance", February 16, 2023, https://www.osc.state.ny.us/state-agencies/audits/2023/02/16/artificial-intelligence-governance

733 R. Abraham, "AI Use by Cops, Child Services In NYC Is a Mess: Report

says", Vice, February 22, 2023, https://www.vice.com/en/article/3adxak/nypd-child-services-ai-facial-recognition

734 Office of the New York State Comptroller, Division of State Government Accountability, "Artificial Intelligence Governance: Report 2021-N-10", February 2023, https://www.osc.state.ny.us/files/state-agencies/audits/pdf/sga-2023-21n10.pdf

735 E. Manis et al., "Scan city - A Decade of NYPD Facial Recognition Abuse", Surveillance Technology Oversight Project (STOP), July 8, 2021, https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/60e5dd3bed032877ec8e3be9/1625677116317/2021.7.7_Scan+City_FINAL.pdf

736 Amnesty International, "Inside NYPD's Surveillance Machine", https://banthescan.amnesty.org/decode/

737 The New York Police Department, "Body-Worn Cameras - What you need to know", https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/body-worn-cameras.page

738 The New York Police Department, "NYPD Questions and Answers - Facial Recognition", https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

739 Ibid.

740 Surveillance Technology Oversight Project (STOP), "NYPD Facial Recognition Lawsuit", https://www.stopspying.org/nypd-facial-rec

741 C. Haskins, "The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI", BuzzFeed, April 6, 2021, https://www.buzzfeednews.com/article/carolinehaskins1/nypd-has-misled-public-about-clearview-ai-use

742 R. Mac et al., "Surveillance Nation", BuzzFeed, April 6, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition

743 A. Perala, "Judge Orders NYPD to Release Biometric Surveillance Docs", FindBiometrics, August 2, 2022, https://findbiometrics.com/judge-orders-nypd-to-release-biometric-surveillance-docs-508021/

744 S. Fussel, "The NYPD Had a Secret Fund for Surveillance Tools", Wired, August 10, 2021, https://www.wired.com/story/nypd-secret-fund-surveillance-tools/

745 Ibid.

746 J. Goldstein, A. Watkins, "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database", The New York Times, August 1, 2019, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html

747 New York Civil Liberties Union (NYCLU), "Stop and Frisk Data", https://www.nyclu.org/en/stop-and-frisk-data

748 New York Civil Liberties Union (NYCLU), "Stop and Frisk in the de Blasio era", March 14, 2019, https://www.nyclu.org/en/publications/stop-and-frisk-de-blasio-era-2019

749 MIT Media Lab, "Gender Shades", "Results", https://www.media.mit.edu/pro-

jects/gender-shades/results/

750 Amnesty International, "USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research", February 15, 2022, https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/

751 Ibid.

752 S. Goldenberg, J. Anuta, "Adams eyes expansion of highly controversial police surveillance technology", Politico, February 8, 2022, https://www.politico.com/news/2022/02/08/adams-police-surveillance-technology-00006230

753 C. Garvie, "Garbage in, Garbage out: Face Recognition on Flawed Data", Georgetown Law Center on Privacy and Technology, May 16, 2019, https://www.flawedfacedata.com/

754 The Surveillance Technology Oversight Project (S.T.O.P.) is a non-profit advocacy organisation and legal services provider working to abolish local governments' systems of mass surveillance

755 T. Ryan-Mosley, "A new map of NYC's cameras shows more surveillance in Black and brown neighborhoods", MIT Technology Review, February 14, 2022, https://www.technologyreview.com/2022/02/14/1045333/map-nyc-cameras-surveillance-bias-facial-recognition/

756 G. Joseph, J. Offenhartz, "NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment", Gothamist, August 14, 2020, https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment

757 J. Offenhartz et al., "The NYPD Banged On A Black Lives Matter Organizer's Door, Shut Down His Street, Stayed For 5 Hours, Then Left", Gothamist, August 7, 2020, https://gothamist.com/news/nypd-banged-black-lives-matter-organizers-door-shut-down-his-street-stayed-5-hours-then-left

758 J. Offenhartz, "Black Activist Targeted In Military-Style NYPD Siege Files Federal Lawsuit", Gothamist, November 4, 2021, https://gothamist.com/news/black-activist-targeted-military-style-nypd-siege-files-federal-lawsuit

759 S. Fussel, "The NYPD Had a Secret Fund for Surveillance Tools", Wired, August 10, 2021, https://www.wired.com/story/nypd-secret-fund-surveillance-tools/

760 The Local, "UPDATE: EU postpones launch of EES border entry system once again", January 19, 2023, https://www.thelocal.no/20230119/update-eu-postpones-launch-of-ees-border-entry-system-once-again

761 F. Giandana Gigena, "Cross-border Surveillance Poses a Silent Threat to Migrants", El Faro, April 24, 2023, https://elfaro.net/en/202304/opinion/26819/Cross-border-Surveillance-Poses-a-Silent-Threat-to-Migrants.htm

762 J. Askew, "'Mass surveillance, automated suspicion, extreme power': How tech is shaping EU borders", Euronews, April 6, 2023, https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders

763 P. Williams, E. Kind, "Data Driven Profiling", European Network Against Racism (ENAR), November 2019, https://www.statewatch.org/media/documents/

news/2019/nov/data-driven-profiling-web-final.pdf

764 D. Bigo, "Globalized (in)security: The field and the ban-opticon", in D. Bigo and A. Tsoukala (eds.), Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11, Routledge, 2008, pp. 10-48

765 D. Bigo, "Security, exception, ban and surveillance", in D. Lyon (ed.), Theorizing Surveillance, Routledge, 2006, pp. 46-68

766 M. Higgins, "How the $68 Billion Border Surveillance Industrial Complex Affects Us All", Vice, June 11, 2021, https://www.vice.com/en/article/k7873m/how-the-dollar68-billion-border-surveillance-industrial-complex-affects-us-all

767 J. Askew, "'Mass surveillance, automated suspicion, extreme power': How tech is shaping EU borders", Euronews, April 6, 2023, https://www.euronews.com/next/2023/04/06/mass-surveillance-automated-suspicion-extreme-power-how-tech-is-shaping-the-eus-borders

768 11.11.11., "Over 200,000 illegal pushbacks at EU's external borders in 2022", March 22, 2023, https://pers.11.be/translation-over-200000-illegal-push-backs-at-eus-external-borders-in-2022

769 A. Fotiadis, I. Papangeli, S. Malichudis, "Asylum Surveillance Systems Launched in Greece without Data Safeguards", BIRN, September 9, 2022, https://balkaninsight.com/2022/09/09/asylum-surveillance-systems-launched-in-greece-without-data-safeguards/

770 Homo Digitalis, "A major success for civil society in Greece: The Hellenic DPA launches an investigation into the Ministry of Immigration and Asylum re the YPERION and KENTAYROS IT systems", March 9, 2022, https://www.homodigitalis.gr/en/posts/11024

771 Homo Digitalis, "The Hellenic Coast Guard wants to acquire social media monitoring software: The Hellenic DPA is urged to exercise its investigative and supervisory powers", February 15, 2022, https://www.homodigitalis.gr/en/posts/10848

772 Hungarian Helsinki Committee, "Hungary: Access to the territory and push backs", Asylum Migration Database (AIDA), April 19, 2023, https://asylumineurope.org/reports/country/hungary/asylum-procedure/access-procedure-and-registration/access-territory-and-push-backs/

773 Human Rights Watch, "Croatia: Ongoing, Violent Border Pushbacks", May 3, 2023, https://www.hrw.org/news/2023/05/03/croatia-ongoing-violent-border-pushbacks

774 Refugees International, "Letter: The EU AI Act must protect people on the move", December 6, 2022, https://www.refugeesinternational.org/reports/2022/12/5/letter-the-eu-ai-act-must-protect-people-on-the-move

775 Border Violence Monitoring Network, "AI Act: European Parliament Endorses Protections Against AI in Migration", May 11, 2023, https://borderviolence.eu/app/uploads/PR-AI-ACT-PICUM-and-BVMN-v2.pdf

776 K. Weitzberg, "Biometrics and counter-terrorism: Case study of Israel/Palestine", Privacy International, May 2021, https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel_Palestine%20v7.pdf

777 M. Cohn, "Israel Is Using a Vast Network of Biometric Cameras to Terrorize Palestinians", Thuthout, May 5, 2023, https://truthout.org/articles/israel-is-using-a-vast-network-of-biometric-cameras-to-terrorize-palestinians/

778 Amnesty International, "Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians In The OPT", May 2, 2023, https://www.amnesty.org/en/documents/mde15/6701/2023/en/

779 Amnesty International, "Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid", May 2, 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

780 A. Ziv, "This Israeli Face-recognition Startup Is Secretly Tracking Palestinians", Haaertz, July 15, 2019, https://www.haaretz.com/israel-news/business/2019-07-15/ty-article/.premium/this-israeli-face-recognition-startup-is-secretly-tracking-palestinians/0000017f-f47b-ddde-abff-fc7fe25c0000?utm_source=pocket_saves

781 A. Ziv, "Israel uses new surveillance technology to distance itself from the occupation. It's not working", Forward, November 30, 2021, https://forward.com/opinion/478846/israel-new-surveillance-technology-occupation-palestinians/

782 Amnesty International, "Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians In The OPT", May 2, 2023, https://www.amnesty.org/en/documents/mde15/6701/2023/en/

783 The non-refoulement principle prohibits countries receiving asylum seekers from removing those individuals from their jurisdiction or effective control when there are substantial grounds for believing that the person would be at risk of irreparable harm upon return.

784 A. Erfani, M. Garcia, "Pushing Back Protection – How Offshoring and Externalization Imperil the Right to Asylum", National Immigrant Justice Centre, FWD.us, August 3, 2021, https://immigrantjustice.org/research-items/off-shoring-asylum

785 Ibid.

786 Ibid.

787 Statement of Cooperation between the Secretariat of Governance of the United Mexican States, National Migration Institute and the Department of Homeland Security for the United States of America concerning Biometric Immigration Information Sharing, January 18, 2017 https://r3d.mx/wp-content/uploads/SOC-2017.pdf

788 United States Department of Homeland Security, "Fact sheet: DHS Agreements with Guatemala, Honduras and El Salvador", https://www.dhs.gov/sites/default/files/publications/19_1028_opa_factsheet-northern-central-america-agreements_v2.pdf

789 United States Department of Homeland Security, "DHS/ALL/PIA-095 International Biometric Information Sharing Program (IBIS)", November 2022, https://www.dhs.gov/publication/dhsallpia-095-international-biometric-information-sharing-program-ibis

790 Access Now, "Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data", March 23, 2023, https://www.accessnow.org/

press-release/statement-terminate-agreements-biometric-data-migrants/

791 Ibid.

792 Ibid.

793 J. Franzblau, "Caught in the Web – The Role of Transnational Data Sharing in the U.S. Immigration System", National Immigrant Justice Center, December 2002, https://immigrantjustice.org/sites/default/files/content-type/research-item/documents/2022-12/NIJC_Policy_Brief_Foreign_data_sharing_December-2022.pdf

794 J. Franzblau, "Caught in the Web – The Role of Transnational Data Sharing in the US Immigration System", National Immigrant Justice Center, Decembr 2022, https://immigrantjustice.org/sites/default/files/content-type/research-item/documents/2022-12/NIJC_Policy_Brief_Foreign_data_sharing_December-2022.pdf

795 It is the only break in the 30,000 km long Pan-American highway (stretching from Alaska to Argentina).

796 D. Wolfe, "The Darién Gap: migrant route of last resort", World Vision, August 8, 2023, https://www.worldvision.ca/stories/child-protection/darien-gap-migrant-route

797 Statement of Jean Gough, UNICEF director for Latin America and the Caribbean, taken from: D. Wolfe, "The Darién Gap: migrant route of last resort", World Vision, August 8, 2023, https://www.worldvision.ca/stories/child-protection/darien-gap-migrant-route

798 J. Shute, S. Townsley, "The 'road of death': A treacherous, jungle trafficking route lined with rotting corpses", The Telegraph, October 17, 2022, https://www.telegraph.co.uk/global-health/climate-and-people/darien-gap-migration/

799 Office of the United Nations High Commissioner for Human Rights, "Guiding Principles on Business and Human Rights", 2011, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

800 J. Davidson, "Calls for privacy law reform after Bunnings facial recognition scandal", Financial Review, June 20, 2022, https://www.afr.com/technology/calls-for-privacy-law-reform-after-bunnings-facial-recognition-scandal-20220617-p5aume

801 J. Blakkarly, "Kmart, Bunnings and The Good Guys using facial recognition technology in stores", CHOICE, July 12, 2022, https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store

802 A. Pereira, "Complaint to OAIC on use of facial recognition in retail stores", CHOICE, June 2022, https://www.choice.com.au/consumer-advocacy/policy/policy-submissions/2022/june/complaint-oaic-on-use-of-facial-recognition

803 J. Taylor, "Bunnings and Kmart halt use of facial recognition technology in stores as privacy watchdog investigates", The Guardian, July 25, 2022, https://www.theguardian.com/technology/2022/jul/25/bunnings-and-kmart-halt-use-of-facial-recognition-in-stores-as-australian-privacy-watchdog-investigates

804 J. Nadel, "Bunnings and Kmart facial recognition probe set to finish by July", IT News, February 14, 2023, https://www.itnews.com.au/news/bunnings-and-kmart-facial-recognition-probe-set-to-finish-by-july-590881

805 A. Barbaschow, "The Good Guys Says It's No Longer Trialling Facial Recognition Tech", Gizmodo, July 1, 2022, https://www.gizmodo.com.au/2022/07/the-good-guys-facial-recognition/

806 R. Crozier, "7-Eleven disables facial image capture on customer feedback tablets", IT News, October 14, 2021, https://www.itnews.com.au/news/7-eleven-disables-facial-image-capture-on-customer-feedback-tablets-571272

807 J. Dastin, "Amazon extends moratorium on police use of facial recognition software", Reuters, March 18, 2021, https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

808 J. Nash, "New Amazon biometric-scan cases in media-saturated NYC could add to tech opposition", Biometric Update, March 20, 2023, https://www.biometricupdate.com/202303/new-amazon-biometric-scan-cases-in-media-saturated-nyc-could-add-to-tech-opposition

809 C. Douglas Moran, S. Silverstein, "As self-checkout expands in grocery, here are 4 ways the technology is leveling up", Grocery Dive, March 14, 2022, https://www.grocerydive.com/news/as-self-checkout-expands-in-grocery-here-are-4-ways-the-technology-is-leve/620122/

810 S. Mitchell, "Retailers' blind spot over facial recognition technology", The Australian Financial Review, September 29, 2022, https://www.afr.com/companies/retail/retailers-blind-spot-over-facial-recognition-technology-20220927-p5blc8

811 K. Hill, "How Target Figured Out A Teen Girl Was Preagnant Before Her Father Did", Forbes, February 16, 2012, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=8caa89b66686

812 R. Raj, "Let's Get (Not Too) Personal; When Hyper-personalization Turns From Cool To Creepy", Analytics India Mag, December 9, 2019, https://analyticsindiamag.com/lets-get-not-too-personal-when-hyper-personalization-turns-from-cool-to-creepy/

813 S. Clark, "When Hyper-Personalization Becomes Hyper-Creepy", CMSWire, December 7, 2021, https://www.cmswire.com/customer-experience/when-hyper-personalization-becomes-hyper-creepy/

814 T. Claburn, "Apple Sued in Nightmare Case Involving Teen Wrongly Accused of Shoplifting, Driver's Permit Used By Impostor, and Unreliable Facial-Rec Tech", The Register, May 29, 2021, https://www.theregister.com/2021/05/29/apple_sis_lawsuit/

815 United States District Court of Massachusetts, "Bah v. Apple Inc. and Security Industry Specialists, Inc.", 1:21-cv-10897-RGS, 2021, https://regmedia.co.uk/2021/05/29/pacer_bah_apple.pdf

816 J. Grierson, "Facial recognition cameras in UK retail chain challenged by privacy group", The Guardian, July 26, 2022, https://www.theguardian.com/world/2022/jul/26/facial-recognition-cameras-in-uk-retail-chain-challenged-by-privacy-group

817 Vision Labs, “Luna Platform”, https://visionlabs.ai/solutions/luna-platform/

818 Fight for the Future, “Ban Facial Recognition In Stores”, https://www.banfacialrecognition.com/stores/#scorecard

819 C. Burt, “Facial recognition deployed in convenience stores in Mexico, England, Singapore”, Biometric Update, December 14, 2020, https://www.biometricupdate.com/202012/facial-recognition-deployed-in-convenience-stores-in-mexico-england-singapore

820 Asian Banking and Finance, “Thailand embraces facial recognition tech for e-KYC”, May 10, 2019, https://asianbankingandfinance.net/retail-banking/news/thailand-embraces-facial-recognition-tech-e-kyc

821 NDID, “Services”, https://www.ndid.co.th/service/

822 F. Hersey, “Thailand’s NDID partners with Mastercard to connect digital IDs internationally”, Biometric Update, March 10, 2022, https://www.biometricupdate.com/202203/thailands-ndid-partners-with-mastercard-to-connect-digital-ids-internationally

823 Bangkok Post, “Thailand’s digital GDP skyrockets to B2tn in 2021”, November 3, 2022, https://www.bangkokpost.com/tech/2428640/thailands-digital-gdp-skyrockets-to-b2tn-in-2021

824 UBS, “Единая биометрическая система”, https://bio.rt.ru/about/

825 M. N. Zakirov, “Application of biometric face identification technologies in financial institutions”, Biometric Update, February 5, 2023, https://www.biometricupdate.com/202302/application-of-biometric-face-identification-technologies-in-financial-institutions

826 A. Mascellino, “Russia pushing Unified Biometric System to enter secure facilities”, Biometric Update, August 8, 2022, https://www.biometricupdate.com/202208/russia-pushing-unified-biometric-system-to-enter-secure-facilities

827 A. Macdonald, “Russian pols OK bill to make banks share client biometrics with government”, Biometric Update, July 7, 2022, https://www.biometricupdate.com/202207/russian-pols-ok-bill-to-make-banks-share-client-biometrics-with-government

828 J. Nash, “Russia offers carrots to consolidate biometrics systems under government control”, Biometric Update, January 20, 2022, https://www.biometricupdate.com/202201/russia-offers-carrots-to-consolidate-biometrics-systems-under-government-control

829 L. Matsakis, “Scraping the Web Is a Powerful Tool. Clearview AI Abused It”, Wired, January 25, 2020, https://www.wired.com/story/clearview-ai-scraping-web/

830 NOYB, “€20 Mio fine for Clearview AI in Italy”, March 10, 2022, https://noyb.eu/en/eu-20-mio-fine-clearview-ai-italy

831 NOYB, “Second €20 Mio fine for Clearview AI”, July 13, 2022 https://noyb.eu/en/second-eu-20-mio-fine-clearview-ai

832 CNIL, “Facial recognition: 20 million euros penalty against Clearview AI”, October 20, 2022, https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

833 Privacy International, "Get out our faces, Clearview AI", https://privacyinternational.org/campaigns/get-out-our-face-clearview

834 CNIL, "Facial recognition: the CNIL imposes a penalty payment to Clearview AI", 10 May, 2023, available at: https://web.archive.org/web/20230614161044/https://www.cnil.fr/en/facial-recognition-cnil-imposes-penalty-payment-clearview-ai

835 NOYB, "Clearview AI data use deemed illegal in Austria, however no fine issued", May 10, 2023, https://noyb.eu/en/clearview-ai-data-use-deemed-illegal-austria-however-no-fine-issued

836 A. Robertson, "Clearview AI agrees to permanent ban on selling facial recognition to private companies", The Verge, May 9, 2022, https://www.theverge.com/2022/5/9/23063952/clearview-ai-aclu-settlement-illinois-bipa-injunction-private-companies

837 J. Axelrod, "Government Relies on Industry for Facial Recognition Technology", Bloomberg Law, July 19, 2022, https://news.bloomberglaw.com/privacy-and-data-security/government-relies-on-industry-for-facial-recognition-technology

838 K. Zidan, "The Qatar World Cup Ushers in a New Era of Digital Authoritarianism in Sports", The Nation, December 8, 2022, https://www.thenation.com/article/society/qatar-world-cup-surveillance/

839 L. Foroudi, "France looks to AI-powered surveillance to secure Olympics", Reuters, March 23, 2023, https://www.reuters.com/technology/france-looks-ai-powered-surveillance-secure-olympics-2023-03-23/

840 A. Holland Michel, "Stadiums Have Gotten Downright Dystopian", The Atlantic, February 27, 2023, https://www.theatlantic.com/technology/archive/2023/02/sports-stadiums-security-facial-recognition-surveillance-technology/673215/

841 France 24, "Qatar's ground control on alert for World Cup disasters", August 12, 2022, https://www.france24.com/en/live-news/20220812-qatar-s-ground-control-on-alert-for-world-cup-disasters

842 C. J. Bennett, K. Haggerty (eds.), Security Games: Surveillance and Control at Mega-Events, Routledge, 2011, p. 5

843 M. Wesfreid, "Paris 2024 : pas de reconnaissance faciale aux JO", Le Parisien, November 23, 2022, https://www.leparisien.fr/politique/paris-2024-pas-de-reconnaissance-faciale-aux-jo-23-11-2022-4E3FP2XBWZC4LBY3B4UMPA3QPE.php?ts=1669200293918 (in French)

844 N. Lomas, "French parliament votes for biometric surveillance at Paris Olympics", TechCrunch, March 24, 2023, https://techcrunch.com/2023/03/24/paris-olympics-biometrics-surveillance/

845 MEP Patrick Breyer, "Vote to stop a future of biometric mass surveillance in Europe!", Patrick-Breyer.de, March 17, 2023, https://www.patrick-breyer.de/wp-content/uploads/2023/03/MEP-letter-to-FR-MPs-about-biometric-mass-surveillance-in-2024-Olympic-law.pdf

846 La Quadrature du Net, "France Becomes The First European Country To Legalize Biometric Surveillance", March 29, 2023, https://www.laquadrature.net/en/2023/03/29/france-becomes-the-first-european-country-to-legalize-biometric-surveillance/

847 A. Lodie, S. Celis Juarez, "Ai-Assisted Security At The Paris 2024 Olympic Games: From Facial Recognition To Smart Video", AI Regulation, January 27, 2023, https://ai-regulation.com/ai-driven-systems-paris-olympics/

848 C. Whelan, "Surveillance, security and sporting mega events: Toward a research agenda on the organisation of security networks", Surveillance and Society 11(4): Surveillance and Sport, 392-404, 2014, http://dx.doi.org/10.24908/ss.v11i4.4722, p. 393

849 M. Viegas Ferrari, "Test, swarm, normalize: how surveillance technologies have infiltrated Paris 2024 Olympic Games", Cadernos Metrópole 25(56), 75-96, 2023 http://dx.doi.org/10.1590/2236-9996.2023-5603, p. 83

850 La Quadrature du Net, "General Mobilisation Against The Legalisation Of Algorithmic Video Surveillance!", February 16, 2023, https://www.laquadrature.net/en/2023/02/16/general-mobilisation-against-the-legalisation-of-automatic-video-surveillance/

851 M. Borak, "French top court OKs AI surveillance at Olympics but no biometrics", Biometric Update, May 19, 2023, https://www.biometricupdate.com/202305/french-top-court-oks-ai-surveillance-at-olympics-but-no-biometrics

852 Privacy International, "King's Cross has been watching you - and the police helped", June 25, 2020, https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped

853 Liberty, "Legal Challenge: Ed Bridges V South Wales Police", https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/

854 L. Dearden, "Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested", The Independent, January 31, 2019, https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

855 Big Brother Watch, "Face off: The lawless growth of facial recognition in UK policing", May 2018, https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report/

856 V. Dodd, "Met police found to be institutionally racist, misogynistic and homophobic", The Guardian, March 21, 2023, https://www.theguardian.com/uk-news/2023/mar/21/metropolitan-police-institutionally-racist-misogynistic-homophobic-louise-casey-report

857 Liberty, "Facial Recognition", https://www.libertyhumanrights.org.uk/fundamental/facial-recognition/; Big Brother Watch, "Stop Facial Recognition", https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

858 P. Fussey, D. Murray, "Impact: Report on the police use of facial recognition technology identifies significant concerns", University of Essex, https://www.essex.ac.uk/research/showcase/report-on-the-police-use-of-facial-recognition-technology-identifies-significant-concerns

859 University of Essex, "Impact: Viewing the risks of Artificial Intelligence through a human rights lens", https://www.essex.ac.uk/research/showcase/viewing-the-risks-of-advanced-ai-through-a-human-rights-lens

860 M. Burgess, "Co-op is using facial recognition tech to scan and track shoppers",

Wired, December 10, 2020, https://www.wired.co.uk/article/coop-facial-recognition

861 R. Williams, "Supermarkets in talks to trial age estimation technology for buying alcohol later this year", inews, April 13, 2021, https://inews.co.uk/news/technology/age-estimation-trials-supermarket-alcohol-953540; M. Prendergast, "Yoti digital age verification trialled at supermarkets", techUK, January 6, 2023, https://www.techuk.org/resource/yoti-digital-age-verification-trialled-at-supermarkets.html

862 Meta, "Introducing New Ways to Verify Age on Instagram", June 23, 2022, https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/

863 Privacy International, "The Identity Gatekeepers and the Future of Digital Identity", October 10, 2019, https://privacyinternational.org/long-read/3254/identity-gatekeepers-and-future-digital-identity

864 Biometrics Institute, "Home", https://www.biometricsinstitute.org/

865 IBIS World, "Biometrics Scan Technology Development in the UK - Market Size 2011–2029", March 16, 2023, https://www.ibisworld.com/united-kingdom/market-size/biometrics-scan-technology-development/

866 HR News, "Number of CCTV Cameras in the UK reaches 5.2 million", November 19, 2020, https://hrnews.co.uk/number-of-cctv-cameras-in-the-uk-reaches-5-2-million/

867 Aljazeera, "Head of UK anti-monarchy group arrested at coronation protest", May 6, 2023, https://www.aljazeera.com/news/2023/5/6/head-of-uk-anti-monarchy-group-arrested-at-coronation-protest

868 I. Kottasová, "'It's not a good look.' As cost of living crisis bites, some Brits are questioning spending money on glitzy coronation", CNN, May 2, 2023, https://www.cnn.com/2023/05/02/business/cost-of-living-doncaster-coronation-gbr-cmd-intl/index.html

869 V. Dodd, "Police accused over use of facial recognition at King Charles's coronation", The Guardian, May 3, 2023, https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation

870 Ibid.

871 ECHR, "Guide on the case-law of the European Convention on Human Rights: Mass Protests", August 31, 2022, https://www.echr.coe.int/Documents/Guide_Mass_protests_ENG.pdf

872 European Digital Rights (EDRi), "Ban Biometric Mass Surveillance Explainer", https://edri.org/wp-content/uploads/2020/05/Explainer-Ban-Biometric-Mass-Surveillance.pdf

873 Metropolitan Police, @metpoliceuk, "Our tolerance for any disruption, whether through protest or otherwise, will be low. We will deal robustly with anyone intent on undermining this celebration. ", Twitter, May 3, 2023, https://twitter.com/metpoliceuk/status/1653745710724968448

874 College of Policing, "Changes to legislation for policing protests", July 2, 2023, https://www.college.police.uk/article/changes-legislation-policing-protests

875 Liberty, "How Does The New Policing Act Affect My Protest Rights?", https://

www.libertyhumanrights.org.uk/advice_information/pcsc-policing-act-protest-rights/

876 B. Quinn, R. Sya, V. Dodd, "Anti-monarchists receive 'intimidatory' Home Office letter on new protest laws", The Guardian, May 2, 2023, https://www.theguardian.com/politics/2023/may/02/anti-monarchists-receive-intimidatory-home-office-letter-on-new-protest-laws-coronation

877 M. Hyde, "Yes, the Met police threw royal protesters into cells for no good reason – but at least they regret it", The Guardian, May 9, 2023, https://www.theguardian.com/commentisfree/2023/may/09/met-police-royal-protesters-cells-force

878 UK Surveillance Camera Commissioner's Office, "The Commissioner discusses the new era for live facial recognition after the Coronation", May 17, 2023, https://videosurveillance.blog.gov.uk/2023/05/17/the-commissioner-discusses-the-new-era-for-live-facial-recognition-after-the-coronation/

879 UK Biometrics and Surveillance Camera Commissioner, "Letter from the Biometrics and Surveillance Camera Commissioner to Lucy Allan MP about cameras around MPs' home addresses (accessible)", May 12, 2023, https://www.gov.uk/government/publications/letter-to-lucy-allan-mp-about-cameras-around-mps-home-addresses/letter-from-the-biometrics-and-surveillance-camera-commissioner-to-lucy-allan-mp-about-cameras-around-mps-home-addresses-accessible; UK Biometrics and Surveillance Camera Commissioner, "Biometrics and Surveillance Camera Commissioner: report 2021 to 2022", February 9, 2023, https://www.gov.uk/government/publications/biometrics-and-surveillance-camera-commissioner-report-2021-to-2022

PHOTO CREDITS

p. 15, 228 Photo by Andrew Heald on Unsplash
p. 18 Photo by Steve Johnson on Unsplash
p. 33 Photo by Nathaniel Sison on Unsplash
p. 67, 270 Photo by Rob Curran on Unsplash
p. 72 Photo by Seb on Unsplash
p. 81 Photo by Justin Main on Unsplash
p. 90 Photo by Nuno Alberto on Unsplash
p. 104 Photo by Alev Takil on Unsplash
p. 118 Photo by Atharva Tulsi on Unsplash
p. 128 Photo by Amani Nation on Unsplash
p. 137 Photo by Fabio Alves on Unsplash
p. 146 Photo by Jacques Nel on Unsplash
p. 154 Photo by Ryan Miglinczy on Unsplash
p. 160 Photo by Mavis CW on Unsplash
p. 170 Photo by Stephan Cassara on Unsplash
p. 204 Photo by Tatenda Mapigoti on Unsplash
p. 211, 262 Photo by Maxim Hopman on Unsplash
p. 230 Photo by Saw Wunna on Unsplash
p. 236 Photo by Jack Finnigan on Unsplash
p. 244 Photo by Barbara Zandoval on Unsplash
p.247 EPA/Dimitris Todoris
p. 250 Sophia Goodfriend for foreign policy
p. 252 Photo by Greg Bulla on Unsplash
p. 256 Photo by Egor Litvinov on Unsplash
p.258 Photo by Bernard Hermant on Unsplash
p. 268 Photo by Enrique Alarcon on Unsplash
p. 273 Photo by Adrian Raudaschl on Unsplash

CIP - Каталогизација у публикацији

Народна библиотека Србије, Београд

351.755:57.087.1]:342.72/.73(082)

BEYOND the face : biometrics and society / [edited by Ella Jakubowska, Andrej Petrovski & Danilo Krivokapić]. - Beograd : Share foundation, 2023 (Novi Sad : NS press). - 349 str. : ilustr. ; 21 cm

Tiraž 300. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 278-346. - Iz sadržaja: Technology / Bojan Perkov. Legal / Jelena Adamović & Duje Kozomara. Practical / Mila Bajić & Duje Prkut.

ISBN 978-86-89487-19-0

a) Биометријски системи идентификације -- Право на заштиту података о личности -- Зборници

COBISS.SR-ID 129123337