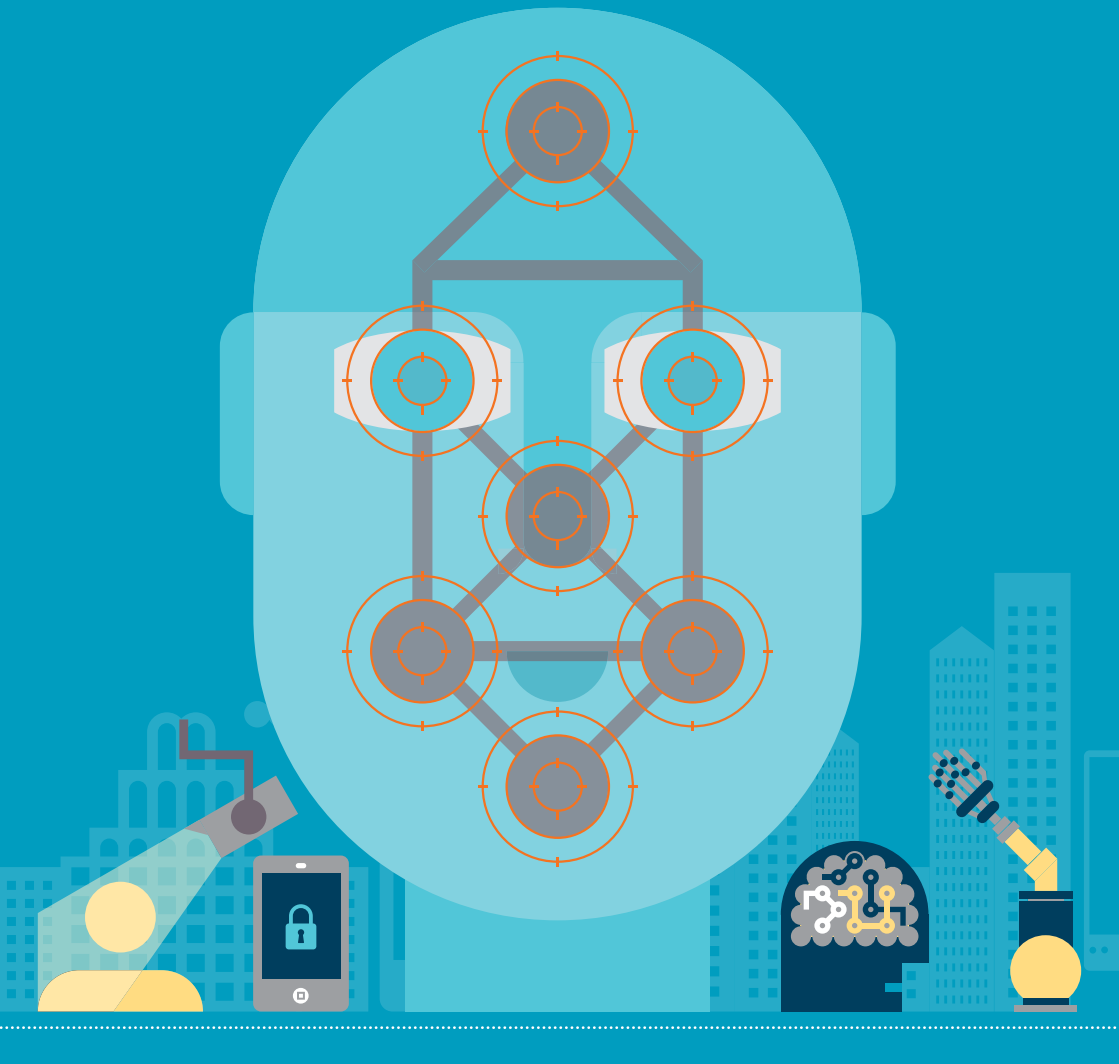
Osborne Clarke

# Automated Facial Recognition

## A UK overview

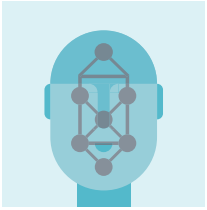


# Are you using AFR?

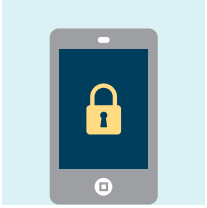
Recent technological advances in artificial intelligence and machine learning have dramatically improved the utility of Automated Facial Recognition technology ("AFR") which is increasingly being deployed in both commercial and state sponsored contexts.

Although facial data is a form of biometric data, it is typically subject to additional layers of regulation. AFR is clearly a topic which has drawn the attention of a number of commentators and has the potential to cause serious reputational damage to a business if it fails to sensitively take into account the wider societal implications of use – let alone the narrower regulatory implications. Recent studies have also indicated that the technology may not be as accurate as initially thought. This makes any use case evaluation of AFR even more important.

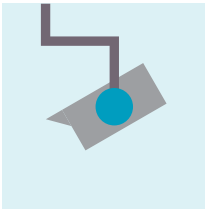
Are you using or likely to use AFR within your business? Has your business proposed rolling out AFR? Take a moment to look at the following use-cases:



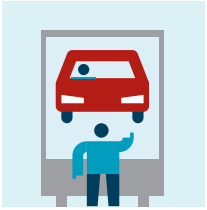
**Automated Building Access/Entry Control**
Many AFR applications are now being used to control access to secure sites and environments, typically replacing token based systems, which rely on physical photo identity cards and RFIDs to open entry ways. As systems become affordable, use is spreading to general entry systems, where AFR is increasingly used for its convenience, rather than because high security is a necessity.



**Device Unlock**
On a similar but device-based level, AFR systems are used to unlock computers and phones – the most commonly deployed being FaceID on Apple's iPhone X which replaces the biometric fingerprint scanning method.

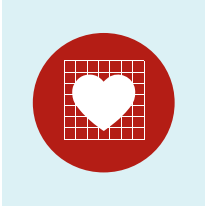


**Crime Prevention and Monitoring**
Major retail establishments across the United States and China are using or considering the deployment of AFR based applications which match facial databases to datasets of individuals with known criminal records for fraud and shoplifting. Coupled with this, of course, is the use of AFR by law enforcement authorities in the fight against crime.



**Smart Advertising**
AFR can be used to target particular audience demographics – recognising whether the person staring at the advert is male, female, old, young, or from a particular ethnic background. More advanced systems are even able to detect different emotional states expressed on an individual's face, helping companies to work out the effectiveness of their advertising.

**Social Media Identification and Classification**
Social media platforms already deploy AFR as part of a network classification exercise, 'tagging' individuals who are identified as existing members of that network and making it easier for other people to search for contacts.



**Medical Diagnosis**
AFR is a valuable tool in the diagnosis of diseases and physical conditions which cause detectable changes in appearance, such as some rare genetic disorders. It is also being used in other situations where insight into health status is useful – for example by insurance underwriters to determine whether a person is a heavy smoker or drinker.

**Cashless Retail and Secure Transactions**
AFR is being used by major online retailers to disrupt traditional "bricks and mortar" cash and card payment models – simply walk into a store, grab an item and leave. On a similar level, AFR can enhance payment security by logging an individual's unique facial features and using them for additional payment authentication with traditional tokenised payments, such as credit and debit cards.

# A legal overview

Whilst it is true to say that the legal position in relation to Automated Facial Recognition is evolving, it is **not** correct to assume that there is no regulation.

By its nature, much of the existing law applicable to AFR is "use case" dependent and will apply differently, for example, if you are using the technology as part of an active video surveillance application, querying a pre-existing facial database, or a combination of both.

Different laws and codes of conduct will apply depending upon the extent to which your facial recognition application is used on public or private property and, of course, state actors such as the police, counter-terrorism and intelligence services will be bound by a separate regime applicable to the covert gathering and use of such data. Each use case will also likely fall under the oversight of a different, or multiple, regulators.

This guide should not be treated as a substitute for proper and directed legal advice. We have however attempted to set out some overarching pointers and essential themes which will assist in developing an understanding of the relevant legal landscape. We have also added a snapshot flowchart which should provide an overview of the key questions which need to be asked in any regulatory evaluation of a specific AFR use case. This guide covers the regulatory position in the UK, as influenced by its European and international treaty obligations.

### 1. Personal Data: The General Data Protection Regulation ("GDPR") and Data Protection Act 2018 ("DPA 2018")

Any analysis of the compliance of your AFR system will inevitably need to start with an assessment of its adherence to the data protection regime under the GDPR and DPA 2018, and relevant guidance issued by the Information Commissioner's Office ("ICO").

Facial images themselves are classed as personal data (i.e. data that can readily identify individuals) but processing by an AFR system, converting it into biometrics, brings with it extra stringent regulation. Issues you will need to consider include ensuring that your application is designed with a view to maintaining privacy (referred to as "privacy by design") and determining the lawful basis upon which you are seeking to use AFR. Understanding how AFR data will be held and processed is vital to determining the legality of your use case. From an AFR perspective you'll also need to be aware of the ICO's guidance on CCTV (the Code of Practice for Surveillance Cameras and Personal Information) if your application involves video surveillance.

### 2. Article 8 of the European Convention on Human Rights ("ECHR") and the Human Rights Act 1998 ("HRA 1998")

Article 8 of the ECHR provides for a right to respect for one's private and family life, home and correspondence and is directly actionable under English law through the mechanism of the HRA 1998. The right is clearly designed to circumscribe and limit intrusive activity which could damage privacy. You'll need to think carefully how your AFR application might interfere with those rights. Current police trials of AFR are subject to challenge by human rights organisations on this basis.

### 3. The Protection of Freedoms Act 2012 ("PFA 2012")

Chapter 2 of Part 1 of the PFA 2012 provides for oversight by the Biometrics Commissioner of certain biometric data gathered under the Police and Criminal Evidence Act 1998 – principally fingerprints, DNA samples and custody pictures but increasingly also facial databases (such as the National Police Database) maintained by law enforcement authorities. Chapter 1 of Part 2 (s33) of the PFA 2012 governs the use and regulation of CCTV and other surveillance camera technology by "relevant authorities" (principally state actors), and provides for the Surveillance Camera Commissioner, see 5. below.

### 4. The Regulation of Investigatory Powers Act 2000 ("RIPA 2000"), the Intelligence Services Act 1994 ("ISA 1994") and Part III of the Police Act 1997 ("PA 1997")

RIPA 2000, ISA 1994 and the PA 1997 together put in place a regulatory framework for state actors, principally around the gathering and retention of covert investigative information, to determine proportionality and necessity, as well as intrusive interference in relation to real property and voice and data networks – by definition this includes the operation of "covert" AFR systems. This guide is not intended to focus on the state-sponsored use of AFR technologies, but you need to be mindful that separate rules exist to cover such use and by definition often permit activities which are beyond mere commercial use. The Investigatory Powers Commissioners Office ("IPCO") has regulatory oversight, as well as the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board.

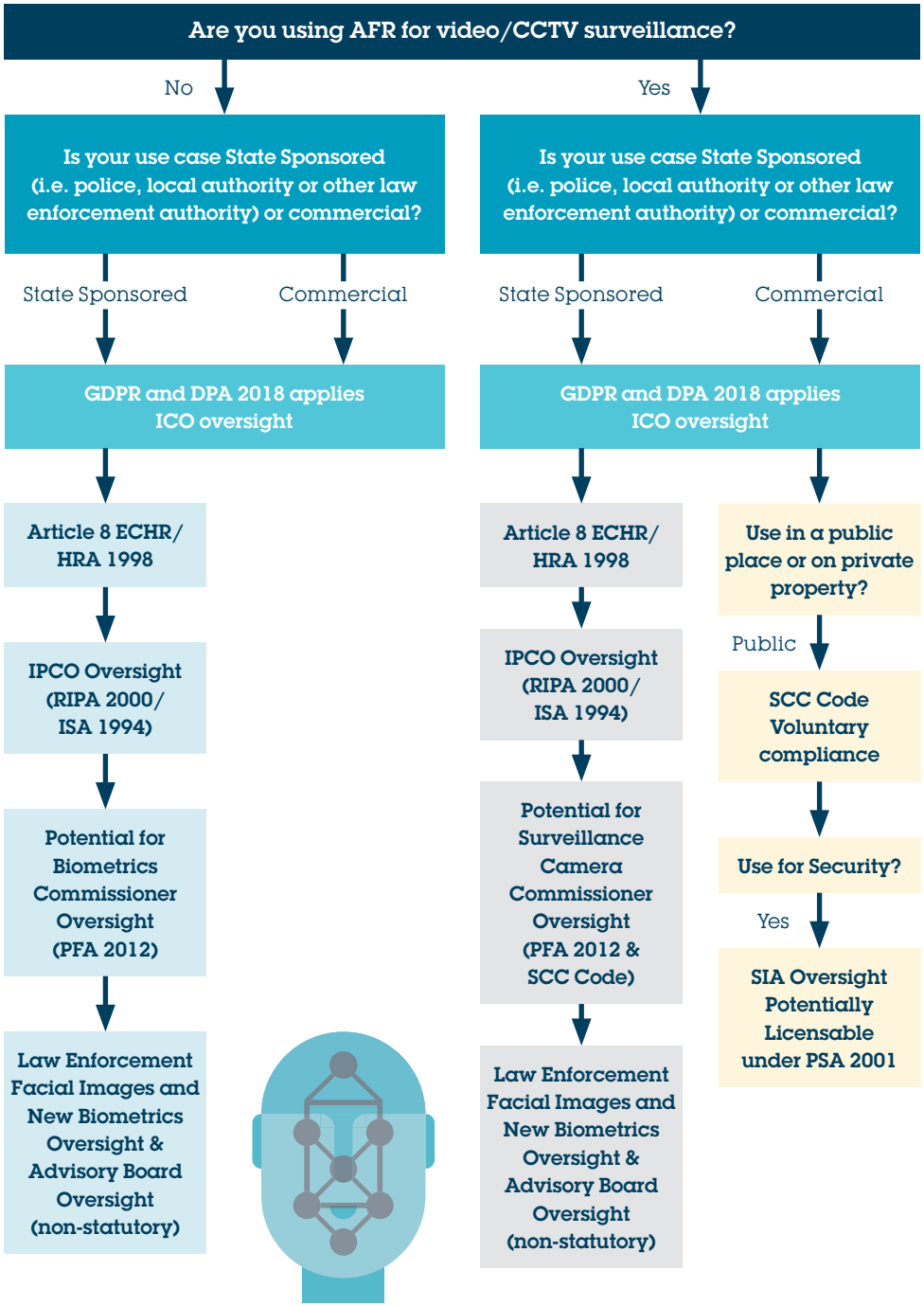
### 5. The Surveillance Camera Code of Practice 2013 ("SCC Code")

The SCC Code applies to the use of "overt" video surveillance systems in public places by relevant public authorities, where compliance is mandatory. Chapter 4 in particular refers to the use and/or processing of images obtained by CCTV (and Principle 12 specifically). The code is administered by the Surveillance Camera Commissioner ("SCC"). Where AFR is used as part of a public authority administered public scheme, the SCC will have jurisdiction and can enforce compliance with the SCC Code. The SCC's mission is to ensure voluntary compliance with the SCC Code by unregulated (private) entities.

### 6. The Private Security Act 2001 ("PSA 2001")

If your AFR application involves a security application which extends to public spaces and which includes CCTV monitoring and/or door supervision, then this may constitute a licensable activity under the PSA 2001. This legislation was originally enacted to provide a licensing regime for the private security industry which had suffered from a poor reputation previously. Licences are administered by the Security Industry Association ("SIA"). Failure to obtain a licence, when one is needed, is a criminal offence which may be punishable by fines and/or imprisonment.

## Regulation in a Snapshot



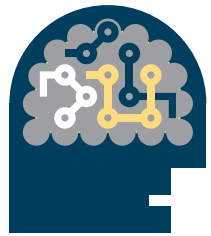

## How we can help

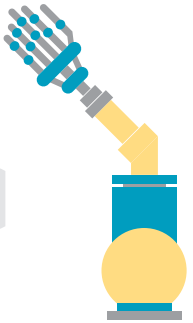
We specialise in advising on the use and development of new and innovative technologies and the disparate and sometimes unintended consequences of complying with multiple overlapping regulatory regimes, often bewildering and rarely clear. Automated Facial Recognition technology is a classic example of this – a powerful new technology which combines AI and machine learning with large amounts of personal biometric data.

We can help you evaluate the correct regulatory steps necessary for your AFR application and if necessary assist with appropriate SIA licences.

Our experts guide enterprises in the digital transformation space, assisting businesses seeking to develop and/ or deploy AFR, Biometrics, AI, Machine Learning and Robotics. Relevant services include:

– Advisory/Regulatory
– Data Protection
– Intellectual Property
– Licensing
– Systems Integration & Development





## Our Experts


**John Buyers – Partner**
**Head of AI and Machine Learning**
T +44 20 7105 7105
john.buyers@osborneclarke.com

**Tamara Quinn – Partner**
**AI, Data Protection and IP**
T +44 207 105 7066
tamara.quinn@osborneclarke.com

**Simon Bollans – Senior Associate**
**AI & Machine Learning**
T +44 207 105 7656
simon.bollans@osborneclarke.com

**Cathy Han – Senior Associate**
**AI & Machine Learning**
T +44 20 7105 7390
cathy.han@osborneclarke.com

**John Jackson – Associate**
**AI & Machine Learning**
M +44 7769 135 011
john.jackson@osborneclarke.com

**Emily Barwell – Associate**
**AI & Machine Learning**
T +44 117 917 3042
emily.barwell@osborneclarke.com

## Osborne Clarke in numbers

**900+**
talented lawyers

working with

**270+**
expert Partners

in

**26**
international locations*

advising across

**8**
core sectors

with

**1**
client-centric culture

## Our locations around the world

**Europe**
Belgium: Brussels
France: Paris
Germany: Berlin, Cologne, Hamburg, Munich
Italy: Brescia, Busto Arsizio, Milan, Rome
The Netherlands: Amsterdam
Spain: Barcelona, Madrid, Zaragoza
UK: Bristol, London, Reading

**USA**
New York, San Francisco, Silicon Valley

**Asia**
China: Shanghai
Hong Kong
India*: Bangalore, Mumbai, New Delhi
Singapore

Osborne Clarke is the business name for an international legal practice and its associated businesses. Full details here: osborneclarke.com/verein/

* Services in India are provided by a relationship firm

**osborneclarke.com**


Publication number O_1907021817DB