

March 2021

# Facial Recognition and Human Rights: Investor Guidance

**CANDRIAM**   
A NEW YORK LIFE INVESTMENTS COMPANY

# About the authors

## Benjamin Chekroun

Stewardship Analyst: Proxy Voting and Engagement



Benjamin Chekroun joined Candriam in 2018 as Deputy Head of Convertible Bonds, assuming his current position in Stewardship in 2020. Previously, he worked at ABN AMRO Investment Solutions since March 2014, where he was in charge of the global convertible bond strategy. He has spent four years in Hong Kong, one year in New York and thirteen years in London, working as a convertible bond trader. In 2004, the fund managed by M. Chekroun was awarded Best Convertible Arbitrage Fund by Hedge Fund Review. Benjamin holds a Masters degree in international business.

## Sophie Deleuze

Lead ESG Analyst, Stewardship



Sophie Deleuze joined Candriam's ESG Research Department in 2005. Following more than a decade as an ESG analyst, she specialized in Candriam's Engagement, Proxy voting, and Stewardship efforts, coordinating our engagement with our ESG analysis and all our investment management teams. Prior to Candriam, she spent four years as an SRI analyst at BMJ CoreRatings, and Aresé. Mme. Deleuze holds an Engineering Degree in Water Treatment, and a Masters in Public Environmental Affairs.

## Quentin Stevenart

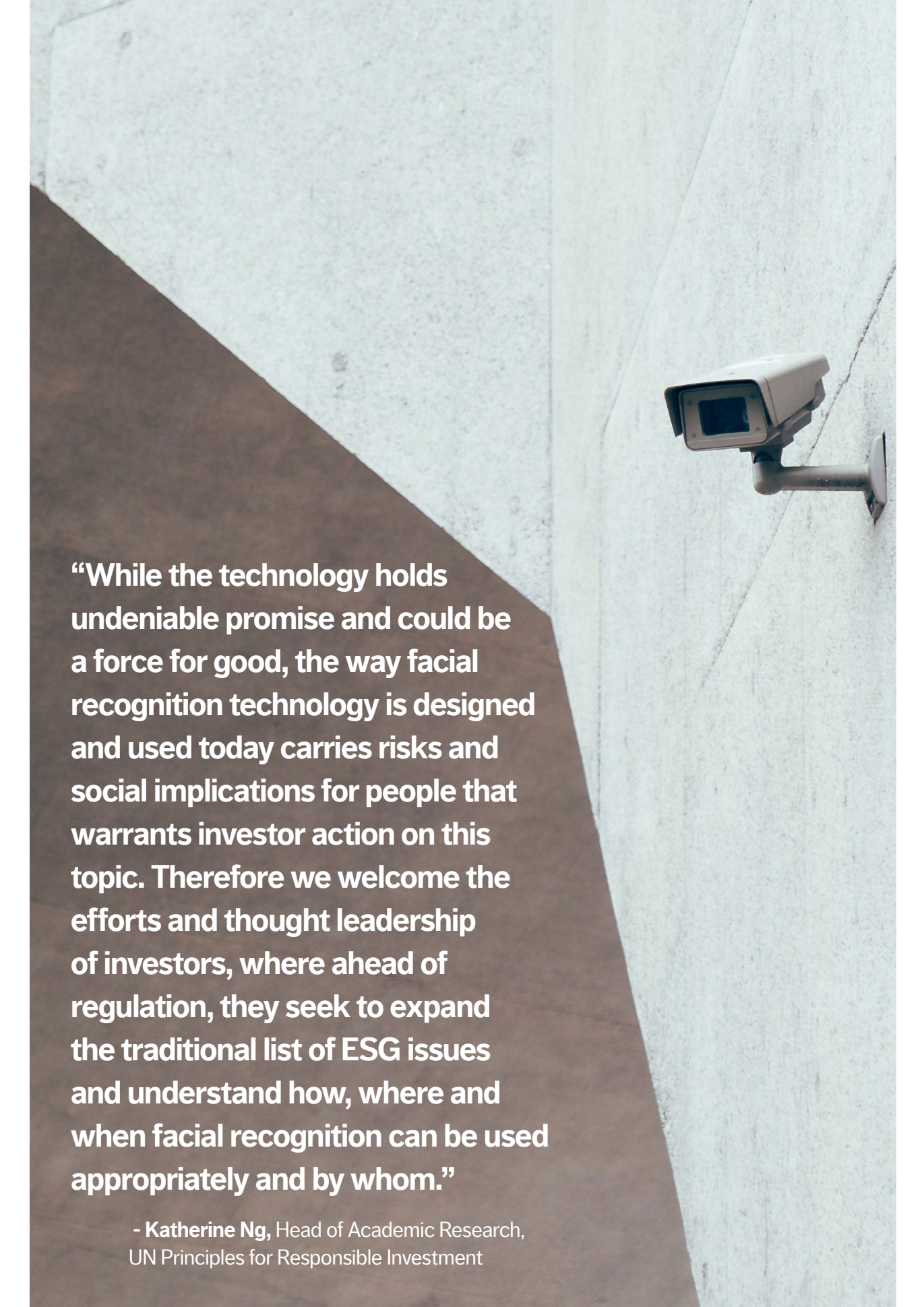
ESG Analyst



Quentin joined Candriam's ESG Team as an ESG Analyst in 2016. He conducts full ESG analysis of the IT sector, and on governance issues across industries. He also coordinates Candriam's Circular Economy research. He holds a Master's degrees in Management from the Louvain School of Management, as well as a Masters and Bachelors in Business Engineering from the Catholic University of Leuven.

# Table of contents

<a href="#">Executive Summary</a>	<b>03</b>	<a href="#">Engagement Practical Guidance</a>	<b>22</b>
<a href="#">The Technology</a>	<b>04</b>	<a href="#">Conclusion</a>	<b>27</b>
<a href="#">Risks and Controversies</a>	<b>10</b>	<a href="#">Notes &amp; References</a>	<b>28</b>



**“While the technology holds undeniable promise and could be a force for good, the way facial recognition technology is designed and used today carries risks and social implications for people that warrants investor action on this topic. Therefore we welcome the efforts and thought leadership of investors, where ahead of regulation, they seek to expand the traditional list of ESG issues and understand how, where and when facial recognition can be used appropriately and by whom.”**

**- Katherine Ng**, Head of Academic Research,  
UN Principles for Responsible Investment

# Executive Summary

***Responsible Investing is more than reacting to the risks and problems we face today. It means thinking beyond carbon footprints and climate change and looking to the risks and opportunities of the future.***

Technology has brought the world some wonderful benefits – and some wonderful investments. Technology has allowed many professional workers to continue their jobs from their homes during the current pandemic. President Biden conducted a significant portion of his election campaign from his basement. Yet we must be aware in any new technology that unintended consequences can arise.

Facial Recognition Technology (FRT) enhances efficiency and security. We use it to unlock high-end smartphones, and to pass through airports. It also has human rights implications. The technology has been under development for decades, but is only now beginning to be broadly used.

A Candriam survey in 2021 generated roughly 300 investor responses. Of these, 30% find Facial Recognition Technology to be a convenient and useful tool. Almost 70% have some reservations – 31% felt FRT is not accurate, while 38% believe that the ethical considerations need to catch up with the technology.

The issues include lack of consent and lack of oversight. Incidents of mis-identification, some resulting in false arrests, are on the rise, especially for non-white citizens. In May 2019, the US city of San Francisco – the birthplace of Facial Recognition – banned its use in law enforcement. Soon after, several large technology companies announced a one-year moratorium on sale of their Facial Recognition products.

To understand the human rights issues which will emerge in the future, responsible investors and other stakeholders should engage today.

*This study could not have been possible without the great help of to following institutions and people. We wish to thank them for their time, insight, and patience:*

- Clare Garvie, *The Center on Privacy & Technology at Georgetown Law*
- Nabylah Abo Dehman, *the United Nations Principles for Responsible Investments*
- Anita Dorett, *The Investor Alliance for Human Rights*
- Isedua Oribhador, *AccessNow*
- Michael Conner, *Open MIC*

# The Technology

---

## How does it Work ?

Facial Recognition is part of the biometric recognition family. It is the process of **identifying** or **verifying the identity** of a person using a picture or a video of their face. It captures, analyses, and compares patterns based on the person's facial details. Some systems now use three-dimensional images for higher accuracy.

There are three main stages to Facial Recognition Technology:

- **Face Detection** is an essential process which detects and locates human faces in images and videos.
- **Face Capture** transforms analogue information -- a face -- into a set of digital information, or data, depicting the facial features of the person. Dozens of facial features such as the spacing of the eyes, bridge of the nose, contours of the lips, ears, chin etc. are measured.
- **Face Matching** verifies whether two faces are the same person.

The algorithm returns a result with a given probability, in a statistical form such as "*Positive match – John Doe - 97.36% Probability*".

## A brief history of Facial Recognition

*Facial Recognition dates back to the 1960s. Woody Bledsoe, a Mormon bishop and co-founder of Panoramic Research in Palo Alto, developed a way to manually input the positions of a person's facial features into a computer. While not very effective by modern standards, it demonstrated that the face was a valid biometric. The accuracy of recognition systems improved in the 1970s as researchers included additional facial markers. Real progress came in the 1980s and 1990s, with new methods to locate a face in an image and extract its features, making fully automated Facial Recognition possible. In 1996 the US FERET Program marked the first build-up of a facial database. The 2001 Super Bowl was the first mass testing of Facial Recognition by law enforcement -- 19 wanted criminals were identified in the crowd. The most dramatic advances were achieved in 2010 and beyond, when deep neural networks improved the technology. In 2011, Facial Recognition technology helped confirm the identity of Osama Bin Laden when he was killed in a US raid. Facebook rolled out the technology for photo tagging and in 2014 its DeepFace program became the first to reach near-human performance in face recognition. In 2017 the iPhone X was the first broadly available smartphone to offer facial unlocking, the first mass release of Facial Recognition technology. In May 2019, San Francisco became the first major US city to ban the use of Facial Recognition by law enforcement agencies. The following summer, IBM CEO pledged to no longer offer IBM FR or analysis software under their 'Principles of Trust and Transparency', followed by major tech giants including Amazon, Facebook, and Microsoft, who have adopted a one-year moratorium on the sale of their products.*

Performing these steps implies the availability and use of certain data and technologies beforehand.

- A Facial Recognition system learns to recognize facial patterns using a **training database** of images. A large, complex and heterogeneous training database is needed for higher accuracy.
- Facial Recognition technology combines the use of **Artificial Intelligence** (the system is capable of learning by analysing data) **Machine Learning** (the system is capable of expanding its ability to process and use information without human intervention, by learning from previous experiences), and **Deep Learning** (a new technique capable of performing machine learning inspired by the way neural networks work inside the human brain).

# Applications

Facial Recognition technology usually performs one or a combination of tasks:



## Identification

“Who are you?”



## Authentication

“Are you really who you say you are?”



## Categorisation

“Which group/category do you belong to ?”

Facial Recognition systems are predominantly used for security and law enforcement but also in the fields of medicine and marketing. The list of applications is expanding rapidly.

- **Law enforcement** -- to locate suspected criminals/terrorists, find a missing person, control access, control a crowd
- **Security** -- to unlock a door/phone/system, validate a transaction, control passengers at an airport
- **Schools** -- for protection, attendance tracking, attention tracking
- **Medicine** -- to diagnose a small but potentially expanding number of diseases, to evaluate pain management
- **Social Media** -- to identify people in pictures
- **Marketing** -- to provide 'SMART' advertising
- **Human to Machine Interaction** -- Autonomous Digital Humans will soon interact with humans and adapt their response according to Facial Recognition.<sup>1</sup>



# Advantages

We all recognise each other not by looking at our fingerprints or the patterns in our irises, but by looking at each other's faces.

Facial Recognition is considered to be the **most natural of all biometric measurements**, because there is no physical interaction required by the end-user. Other signatures of the human body exist, such as fingerprints, iris scans, voice recognition, digitization of veins in the palm, and behavioural measurements, but they are more difficult and cumbersome to implement. Facial recognition is **easily accessible, fast, automatic and seamless**.

Facial recognition systems can process vast amounts of images. For example, the UK police use a system from the Japanese firm NEC called *NeoFace*, which is capable of scanning and identifying as many as 300 faces per second.

**Mistakes, yes...  
...yet Facial  
Recognition  
systems are hard  
to fool.**

*Human rights activists have used social media to demonstrate combinations of hair styles and cosmetics which can be effective in fooling Facial Recognition systems.*

*But not everyone wants to walk around looking like this!*



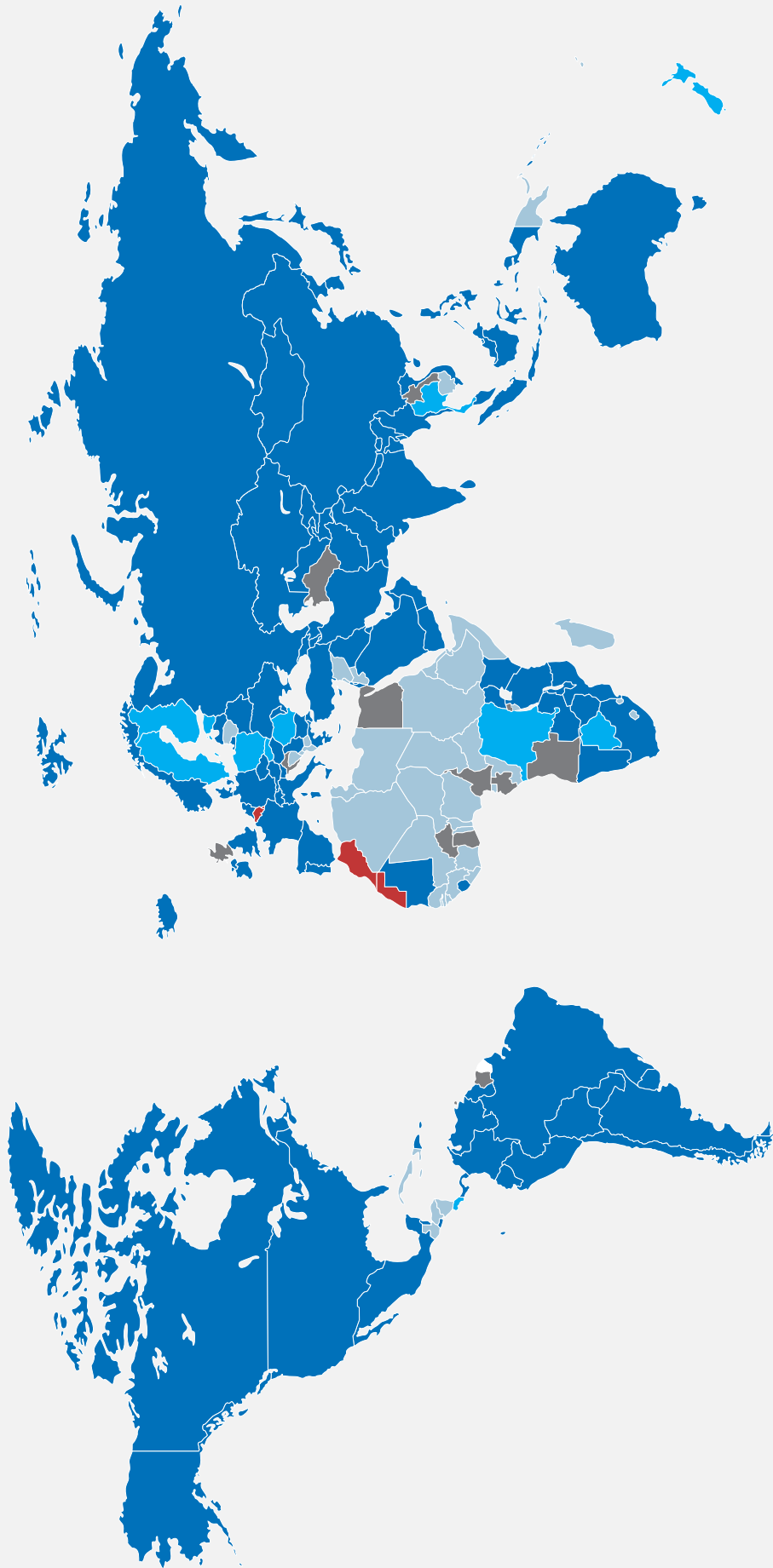
# Facial Recognition – World Presence

The technology is used virtually worldwide, with only modest exceptions. Belgium is one of these exceptions.

**Figure 1:**

The facial recognition world map

- In use
- Approved for use (not implemented)
- Considering technology
- No evidence of use
- Banned

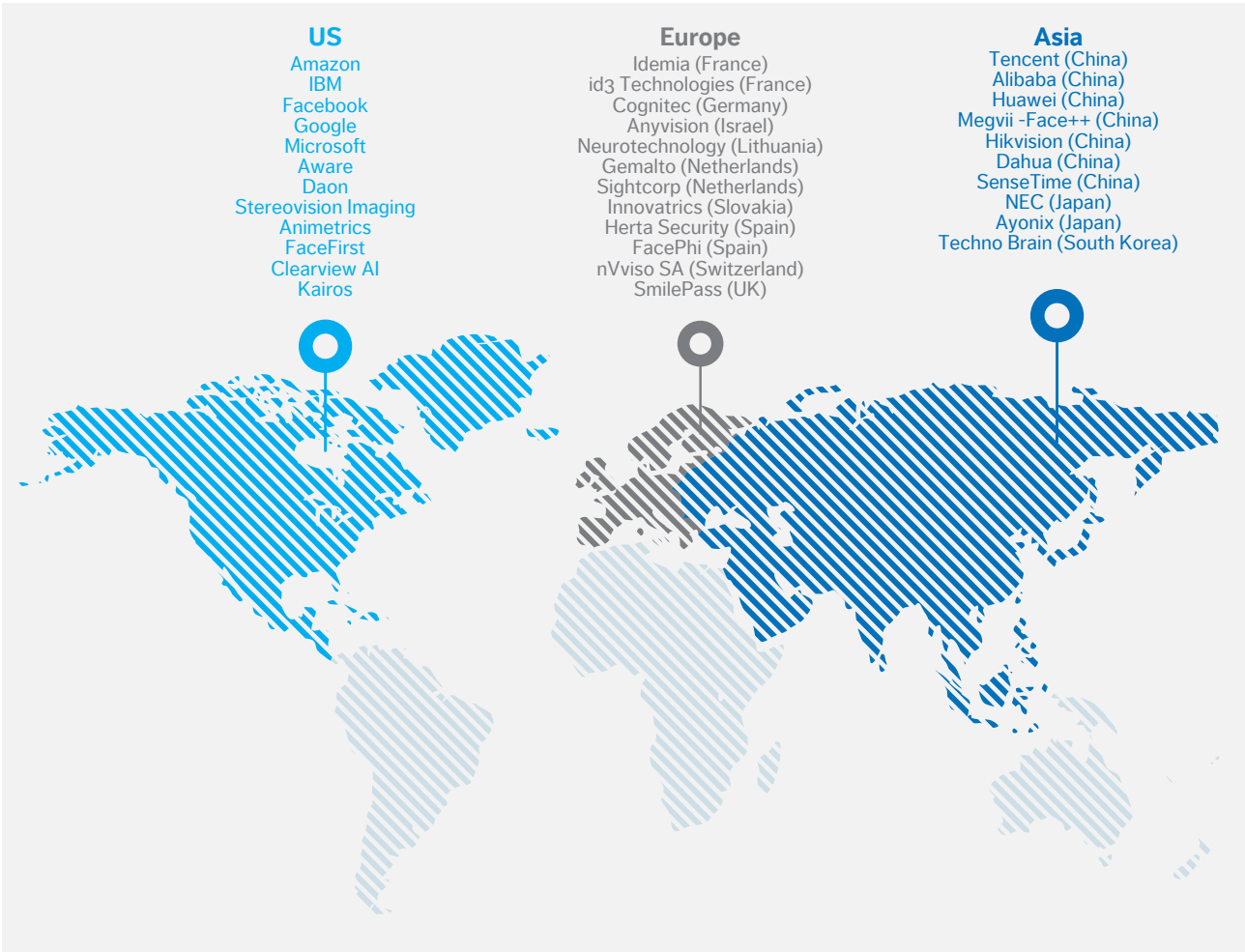


Source: visualcapitalist.com, May 2020; and Candriam

# Market Size and Key Players

According to a 2018 survey by Allied Market Research<sup>2</sup>, the facial recognition market will grow to \$9.6 billion by 2022, an annual **growth rate approaching 25%**. But all things considered, this is a niche sector. It seems some tech giants such as Amazon are including their systems for free as **part of the subscription to more lucrative services**.

**Figure 2:**  
Market Participants



Source: Candriam

# Risks and Controversies

---

Over the past decade, the emergence of Facial Recognition Technology for mass surveillance has brought great concerns to society, along with human rights violations.

## An invasive technology

Facial Recognition surveillance **affects large numbers of us**, in many cases **without our knowledge**, as we go about our daily lives. It can enable surveillance on a mass scale, impinging on our human rights.

It is also true that millions willingly rely on, and welcome, this technology. Many high-level Apple iPhone users rely on 'Face ID' to unlock their smartphones. Millions have registered for automated biometric border control system such as the UK's 'ePassport'.

Across the globe, law enforcement agencies are already deploying Facial Recognition on a massive scale. **It is estimated that one billion surveillance cameras will be in operation by the end of 2021.**<sup>3</sup> China is by far the leading country the use of such system with an estimated 600 million cameras in operation today -- one camera for every 2.3 citizens. Close on its heels comes the US, where an estimated 140 million have been installed -- one camera for every 2.4 citizens. Most of these are digital system whose feeds are exploitable by Facial Recognition systems.

Today, the citizens of Detroit, London, Monaco, Moscow, Beijing and elsewhere are walking around oblivious that their faces are being scanned by police-operated facial recognition systems.

## Accuracy Issues

In January 2020, Robert Williams, a Detroit citizen, was arrested for store theft by the police after being falsely identified, by facial recognition identification.

In 2018 a test of the Amazon technology, *Rekognition*, using members of the US Congress falsely identified 28 congressmen as persons previously arrested for crimes.<sup>4</sup> The test also revealed the racial bias of the technology, as African-American congressmen were disproportionately misidentified as matching the database of arrested persons. One of these was the late Presidential Medal of Freedom winner John Lewis.

Even the most accurate systems available today might make one pause. Imagine a law enforcement agency of a small city using Facial Recognition technology with 99.9% accuracy, where 100,000 people are filmed daily by CCTV. Who is comfortable with 100 people being misidentified every day?

In four years of deployment, since 2016, the London Metropolitan Police's live Facial Recognition surveillance has been 93.59% inaccurate. In two of the three deployments in 2020, the 'Met' had a 100% failure rate - not identifying a single person.<sup>5</sup> The independent review commissioned by the Metropolitan Police also found that their Facial Recognition surveillance was significantly inaccurate. Their analysis looked only at six of the police tests, and found that the Met's accuracy was a mere 19% – that is, inaccurate 81% of the time.<sup>6</sup>

## Why is Facial Recognition, a technology which is bringing more efficiency and security to our everyday lives, also a threat to our human rights?

**Isedua Oribhador, US Policy Analyst at AccessNow:** *“Though facial recognition technology has been touted as a means of improving efficiency and security, we have already seen evidence of the risks that arise from it. From the racial and gender biases baked into these systems, to privacy risks inherent in collecting such personal data, and the potential for enabling mass surveillance of citizens, facial recognition technology poses a severe threat to many fundamental rights. It is imperative to examine these risks and to draw redlines around where use of this technology is incompatible with a respect for human rights.”<sup>7</sup>*

*“Chinese law enforcement agencies have been using a wide-ranging, secret Facial Recognition system to identify, track and control the 11 million Uighurs, a largely Muslim minority.”*



## Country Focus - China

***China's National Intelligence Law of 2017 requires organizations and citizens to “support, assist and cooperate with the state intelligence”. Effectively any software or hardware company in China is required to hand over data to Beijing if authorities express a national security concern.***

Over 200 million surveillance cameras were in use at the end of 2018, with over 600 million estimated in 2020. In the top 10 cities with the most street cameras per person, Chongqing, Shenzhen, Shanghai, Tianjin, and Ji'nan lead the pack.

The Facial Recognition towers in Chinese cities are emblematic of this move. Facial Recognition technology is expanding to Beijing police officers, who now use smart sunglasses which scan faces and report matches.

China's civilian surveillance system is now linked to its “Social Credit System” which rates individuals based on their behaviour. Under this system, which started in 2013, citizens are granted rewards or given punishments depending on their scores.

Chinese police are working with artificial intelligence software companies such as Yitu, Megvii, SenseTime, and CloudWalk. Hardware manufacturers such as Dahua and Hikvision also benefit from large government orders. All of these companies have been added to the US government economic blacklist because of their involvement in the Uighur repression.

Nevertheless, China's ambitions in AI and FR technology remain great. The country aims to become a world leader in AI by 2030. As a government China is clearly the biggest investor in advanced surveillance technologies, AI and FR.

### ***Uighur repression***

Chinese Authorities in the Xinjiang region have been using Facial Recognition technology for racial profiling and surveillance. Chinese law enforcement agencies have been using a wide-ranging, secret Facial Recognition system to identify, track and control the 11 million Uighurs, a largely Muslim minority. Chinese police installed FR scanners at the entrance of several mosques in the region. Xinjiang has been an important testing ground for these firms, where they have been able to operate without the usual constraints



## Gender/Racial Bias, and Stolen Data

The first Facial Recognition experiments were unable to recognise people of African-American or Asian origin. Worse, Google was compelled to apologise in 2015 when its then-new *Google Photos* application labelled some black people as 'gorillas'.

A survey by the MIT Media Lab in 2018 found that some Facial Recognition software could identify a white man with near-perfect precision, but failed spectacularly in identifying darker-skinned women.

Clearview AI states it is working for over 2,400 police agencies in the US. Its CEO, Hoan Ton-That, is linked to far right political movements. Clearview has scraped billions of pictures from Facebook, YouTube and Venmo to build its database.<sup>8</sup> Banjo CEO and founder, Damien Patton, resigned after allegations that he was linked to the Ku Klux Klan. At the time, Banjo had a Facial Recognition service contract worth \$20m with the state of Utah.

Big-tech companies Amazon, Microsoft, and Google parent Alphabet, have all been sued for using photos without the individuals' consent in their development and training of their Facial Recognition technology. Facebook paid a \$650 million settlement for this under the privacy statute of the state of Illinois.<sup>9</sup> Documents leaked by Edward Snowden showed that the National Security Agency in the US has collected millions of facial images. The leaks suggested the photos had been harvested from emails, text messages, social media and video chats.<sup>10</sup>



## **Misuse for private and illegal profit**

Media investigators in Russia found that access to Moscow CCTV live stream was available for sale on the Dark Net by presumably-corrupt police officers. Moscow's city centre has a dense network of 175,000 CCTV cameras, most of which are fitted with Facial Recognition technology. As the system is cloud-based, corrupt officials are able to simply sell their login credentials -- for as little as \$470 -- offering access to the live stream along with the previous five days' recording.

## **Beyond CCTV – Mass Surveillance via Computers, Smartphones, Drones...**

Virtually every new smartphone, personal computer or tablet sold today is equipped with at least one digital camera. Each of these can feed into a Facial Recognition system.

Another concerning development is the deployment of military camera technology on drones, such as the ARGUS-IS, that could allow governments to continuously record areas of up to 10 square miles / 26 square kilometres -- half the size of Manhattan. These systems are capable of scanning the face of any citizen within that radius at any time.<sup>11</sup>

# The Issues

## Lack of Consent

Lack of consent is at the heart of the problem. No company, state, agency or government has asked citizens for their consent. When citizens submit their photo to administrations or agencies to obtain a passport, an ID card or a driving licence, in most jurisdictions they at no point agree to their image being used for Facial Recognition. Other forms of biometric identification imply the consent of the person being checked. Members of the public scanned by live Facial Recognition are unlikely to be aware that they were subject to the identity check, and do not have the opportunity to consent to, or decline, its use.

In Europe the General Data Protection Regulation (GDPR) regulation introduced in 2016 clearly states that biometric data obtained by Facial Recognition technology is personal data. It falls under the protection regulation and therefore requires the consent of the individual for his or her biometric data to be used by any other person, company, or agency. Yet law enforcement agencies in EU countries such as the UK, France, UK, Italy, Greece are already using the technology.

## Lack of Legal Basis

In most countries, there is no legal basis for the police use of live Facial Recognition surveillance. Facial Recognition infringes on basic freedom laws such as the First Amendment of the US Constitution and the Human Rights Act in the UK.

**Clare Garvie, of Georgetown Law's Center on Privacy & Technology, tells Candriam:** "Police use of face recognition in the U.S. remains largely unregulated today, despite state and local efforts to ban its use entirely, and recent revelations that it has led to the arrest of at least three innocent men. In light of the risks it poses to U.S. Constitutional rights to privacy, free speech, fair trials, and equal protection of the laws, face recognition use warrants a moratorium unless and until strong regulation is passed protecting those rights."

## Lack of Oversight

In most countries, such as the US or Europe, we see little evidence of adequate and impartial oversight to control the use of surveillance technology by private companies and law enforcement agencies.

## Disproportionate Intrusion

Multiple tests carried out in the UK have determined that the success ratio has been one wanted criminal identified for every 300,000 faces scanned. The Surveillance Camera Commissioner concluded that the deployment was extremely disproportionate, noting that when “compared to the scale and size of the processing of all people passing a camera, the group they might hope to identify was extremely small”.

## The right to anonymity

A thriving society is built on various freedoms – freedom of expression, of movement, of religion, of association -- but also on the right to reasonable anonymity. Our ability to move through public spaces anonymously is no longer guaranteed because of the wide deployment of Facial Recognition systems. Anyone should be able to walk freely and anonymously. It is part of basic human nature to want to live without looking over one's shoulder. Yet the sphere of life outside of public scrutiny is rapidly vanishing. Being identified by law enforcement, corporates, or governments wherever we go, impedes our individuality. It will ultimately restrict movement, creativity, trust, and even democracy.

As illustration, the London Policing Ethics Panel report on police live Facial Recognition surveillance found that 38% of 16-24 year-olds would stay away from events or places where Facial Recognition surveillance was being used, as well as high numbers of Black, Asian and Minority Ethnic people.<sup>12</sup>

# CAM 3



ID : 254876592

MALE  
BROWN HAIR  
CAUCASIAN  
**STRESSED**



ID  
MA  
GR  
CA  
RE  
BA

**BIOMETRIC IDENTIFICATION : ON - OBJECTS**

10 : 37 : 56

ID : 92548673

FEMALE  
BROWN HAIR  
AFRICAN  
RELAXED  
BAG

ID : 258654892

FEMALE  
CAUCASIAN  
RUNNING  
BAG

: 548765942

MALE  
BROWN HAIR  
CAUCASIAN  
RELAXED  
BAG

SYSTEM  
RECOGNITION  
IN PROGRESS ...

27%

ID : 758426592

FEMALE  
BROWN HAIR  
ASIAN  
RELAXED  
BAG

ID : 458625943

MALE  
CAUCASIAN  
RELAXED  
BAG

DETECTION : ON - BEHAVIOR ANALYSIS : ON

## Is Safety Worth a Little Loss of Privacy ?

When asked how they feel about Facial Recognition, a majority of citizens respond that they understand that to be safer they have to give up a little privacy. The argument of being able to rapidly locate a suspected terrorist or an abducted child strikes a chord.

The surveillance industry exploits fear-based marketing. The fear of terrorist attack, for example. The French city of Nice was the scene of a horrendous attack in 2016 when a terrorist drove a truck through beachfront crowds celebrating Bastille day, killing 87. In response the city equipped the local police with the largest deployment of Facial Recognition and surveillance technology of any French city.

As responsible citizens, we should ask ourselves:

- Do we want to be constantly identified by untested and potentially inaccurate or biased algorithms?
- Do we want our government to record every move we make, every place we visit, and the people we meet?
- Do we want law enforcement to be capable of registering the names of all the participants at a protest march or a religious ceremony?
- Do we want to give our governments unlimited power to watch ***Everyone, Everywhere, All of the Time?***

## A 'Schizophrenic' Society?

When we allow our governments and law enforcement agencies deploy surveillance technology to ensure our safety, we are also saying that for everyone to be safe we need to constantly watch everyone. Some sociologists describe this as a form of schizophrenia.

## Cultural Differences Towards Acceptance of State Surveillance

We cannot just analyse the human rights issues of Facial Recognition through the lens of western values. Perceptions of privacy and intrusion vary greatly among cultures. Most people in China feel that mass surveillance is a normal trade-off for security. In recent years, the combination of mass deployment of surveillance technology with the inception of Social Credit System (box, page 13) has contributed to a dramatic fall in crime rates.

## The Perpetual Line-up

This concept, described by the Centre for Privacy and Technology at Georgetown Law,<sup>13</sup> is that no one would voluntarily take part in a line-up where a victim is going to pick out the criminal! The victim could identify you by mistake. Facial Recognition systems do that every day, pretty much everywhere in the US and China.<sup>14</sup>

## Surveillance Capitalism

In her book 'The Age of Surveillance Capitalism', Shoshana Zuboff defines surveillance capitalism as the process providing free services that billions of people cheerfully use, enabling the providers of those services to monitor the behaviour of those users in astonishing detail -- often without their explicit consent. "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data." Surveillance capitalists are acquiring tremendous financial benefits from the monetisation of individual and collective behavioural data and the predictions of what people are going to do next.

The combination of state surveillance and its capitalist counterpart means that digital technology **is separating the citizens in all societies into two groups, the Watchers -- invisible, unknown and unrestricted -- and the Watched**. This has profound consequences for democracy, because asymmetry of knowledge translates into asymmetries of power. But whereas most democratic societies have at least some degree of oversight of state surveillance, we currently have almost no regulatory control of its privatised counterpart.<sup>15</sup>

# Engagement - Practical Guidance

---

As a responsible investor, our role is to incorporate environmental, social and governance (ESG) factors in our investment decisions, and to practice active ownership. We seek to create long-term value for our clients, by positively impacting the economy, the environment and society as a whole.

It is our conviction that integrating the full picture of Facial Recognition technology in our investments and engagement will contribute to both parts of our goal. An ever-growing number of the companies, states and regions in which we invest are involved in this technology. While we probably would not purposely invest in a pure Facial Recognition issuer, investing in a company using or selling Facial Recognition must involve proper investment due diligence to:

- Assess associated risks
- Share our potential concerns with investees
- Support any changes which help mitigate identified risks



As described in our discussion of the technology and its issues, investor expectations may be numerous, complex, and vary by stakeholder. Some goals follow:

## Corporate Issuers

- **Direct and/or Collaborative engagement** to better understand corporate practices. Expand best practice through conversations with corporates, NGOs, etc.
- **Integrate developments into ESG analysis** of corporates. Define best practices, acceptable progress, and what should constitute an exclusion.
- **Encourage improved corporate behaviours.** Continue to place ethics and respect of human rights at the heart of corporate governance. Establish an independent committee on human rights risk responsible to the Board of Directors. Encourage corporates to choose customers and suppliers aligned with the values they defend.

## Governments

- **Seek suspension of use of Facial Recognition in law enforcement** until specific regulation is established.

## Universities

- **Encourage Ethics classes** in AI/Tech curriculums.

At Candriam, while we plan to discuss this subject with European authorities, we believe our most immediate leverage will be engaging with corporate issuers, and more specifically with companies whose securities we already hold in our portfolios.

Given this perspective, and inspired by exchanges with Facial Recognition specialists/experts, we list below a series of questions that should aid investors in assessing the level of involvement of investee companies in Facial Recognition, as well as capture the associated level of human rights risks.

***Open MIC has been working with shareholders for several years to press tech companies to adopt “ethical” practices regarding facial recognition.***

The Big Tech companies have devoted considerable energy and resources to resisting those efforts. Despite intense shareholder pressure – as well as global pressure from numerous human rights organizations – the companies largely refuse to acknowledge that there is a problem. As the present report highlights, almost all facial recognition products on the market now are operating without the consent of millions of people whose faces are being scanned on a daily basis. Many of those same systems have been found to be racially-biased. There is no recourse or remedy for those whose rights have been violated, contrary to what is required by the United Nations Guiding Principles on Business and Human Rights. In 2019, the UN Special Rapporteur on freedom of opinion and expression recommended “an immediate moratorium on the global sale and transfer of private surveillance technology until rigorous human rights safeguards are put in place.” We have no human rights safeguards in place, yet sales continue. In fact, as this report suggests, it’s a boom market.

One question is whether the prospect of regulation and legislation – in both the EU and the U.S. – will prompt the companies to voluntarily adopt effective industry standards. The firms will doubtlessly lobby to dilute any governmental controls on facial recognition. Investors should definitely continue doing what they’re doing: using all the tools they have to press the tech companies for policies and practices that will make a difference; it will be interesting to see if a large and vocal collaborative engagement, such as the one suggested here, can incite companies to engage in a more productive dialogue.

*Michael Connor is the founding Executive Director of Open MIC, a non-profit that works to foster greater corporate accountability in the media and technology sectors, principally through shareholder engagement. Working with socially responsible investors, Open MIC identifies, develops and supports campaigns that promote values of openness, equity, privacy, and diversity – values that provide long-term benefits for individuals, companies, the economy and the health of democratic society. Open MIC is currently working on campaigns targeting Amazon, Twitter, Google, and Facebook.*

# Engagement Guidance

## Level of involvement

- Does your company provide products (hardware, software, databases) related to Facial Recognition Technology?
- What is the purpose of the product?
  - Surveillance
  - Identification
  - Policing
  - Categorisation (eg, targeted advertising)
  - Investigating
  - Security
  - Other (please specify)
- To what type of users do you provide your Facial Recognition technology?
  - Governments or States
  - Schools
  - Law Enforcement Agencies
  - Corporates
  - Military

## Governance

- Has your company adopted a public-facing policy regarding Facial Recognition technology? If so, what impact has this commitment had
  - 1) on your relationships with business partners, eg suppliers, subcontractors, clients, final users? and
  - 2) on your lobbying activities?
- What risks have you identified in relation to Facial Recognition technology, and how frequently do you report on these to the Board ?
- Does your company conduct human rights impact assessments to identify and assess real and potential human rights risks of your Facial Recognition technologies? What risks have you identified, and which stakeholders have you involved in this assessment? How have you adapted your operations and strategy ? Who in the company (at the corporate / regional / branch level) has the overall and day-to-day responsibility of addressing these specific risks and potential impacts ?

- What processes have you put in place to define which clients you can sell to? Do you ban sales/deliveries of your product or service to certain oppressive/un-democratic countries?

## Management of conception-related risks

- How are you internally organised to identify, prevent and solve Facial Recognition-related risks?

*More specifically :*

- How did your company build/obtain/buy its training database of pictures/names? If you have not constructed the database yourselves, how did your supplier build/obtain/buy the database you use?
- Do you disclose the accuracy of your, and their, technology after measurement by a recognised scientific assessment institution, such as the National Institute of Standards and Technology (NIST)? If not, discuss?
- What internal checks do you have to detect algorithmic bias such as race, gender, or age? And/or your supplier(s)?
- Is there any grievance mechanism in place to identify and compensate persons wrongfully affected by the technology at this level?

## Management of use-related risks

- Are your clients subject to any regulation of their use of Facial Recognition technology? Is this something you track?
- Does your product offer Facial Recognition technology for real time analysis, or retro-active analysis only?
- Does your product analyse live video footage, or static images only?
- Does your Facial Recognition technology product offer any kind of categorisation, eg racial, gender, age, mental, or other?
- Does your Facial Recognition technology product offer any kind of predictive analysis?
- Is there any grievance mechanism in place to identify and compensate persons wrongfully affected by the technology at this level?

# Conclusion

*Today, Facial Recognition is a topic with no transparency. Its use is welcomed by some, controversial for others. It can be misused, and demonstrably exhibits biases and errors.*

*Without transparency, we cannot assess these controversies. To open the door to analysis and conversation, we need more leverage. National and local authorities are beginning to act. Corporations are beginning to act. Momentum and conversation are building among the public, and NGOs are launching campaigns.*

*Now is the time for investors to act.*



# Notes & References

<sup>1</sup> Mashable.com. *Douglas, the latest step toward realistic AI, is unsettling*. Updated 22 November, 2020. <https://mashable.com/article/douglas-realistic-ai-unsettling/?europe=true>, accessed 8 February, 2021.

<sup>2</sup> <https://www.alliedmarketresearch.com/press-release/facial-recognition-market.html>

<sup>3</sup> CNBC. *One billion surveillance cameras will be watching around the world in 2021*. 6 December, 2019. <https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html>, accessed 8 February, 2021.

<sup>4</sup> The American Civil Liberties Union. ACLU.com. Snow, Jacob. *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*. 26 July, 2018. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>, accessed 8 February, 2021.

<sup>5</sup> Metropolitan Police. LIFR Deployments 2020. <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/latest-past-deployment-data.pdf>, accessed 8 February, 2021.

<sup>6</sup> The Human Rights, Big Data and Technology Project. Fussey, Professor Pete and Dr. Daragh Murray. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. July, 2019. <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>, accessed 8 February, 2021.

<sup>7</sup> Isedua Oribhabor is AccessNow's US Policy Analyst, also covering Business and Human Rights. Isedua's work with the Leitner Center for International Law and Justice at Fordham sparked her interest in Business and Human Rights, leading her to pursue the topic as it relates to the technology sector. AccessNow is a global non-governmental organization specializing in the defense on human rights in the field of technology. AccessNow focuses on the following fields: privacy, freedom of expression, digital security, business and human rights and net discrimination. AccessNow has an international presence employing 60 staff across 13 countries.

<sup>8</sup> The New York Times. Hill, Kashmir. *The Secretive Company That Might End Privacy as We Know It*. updated 31 January, 2021. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>, accessed 8 February, 2021.

<sup>9</sup> CNET News. Musil, Steven. *Amazon, Google, Microsoft sued over photos in facial recognition database*. 14 July, 2020. <https://www.cnet.com/news/amazon-google-and-microsoft-sued-over-photos-in-facial-recognition-database/>, accessed 8 February, 2021.

<sup>10</sup> The New York Times. Risen, James and Laura Poitras. *N.S.A. Collecting Millions of Faces From Web Images*. 31 May, 2014. <https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html>, accessed 8 February, 2021.

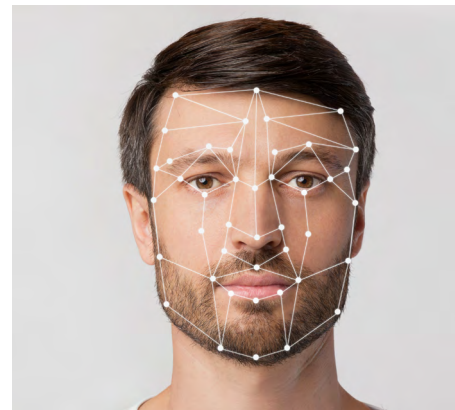
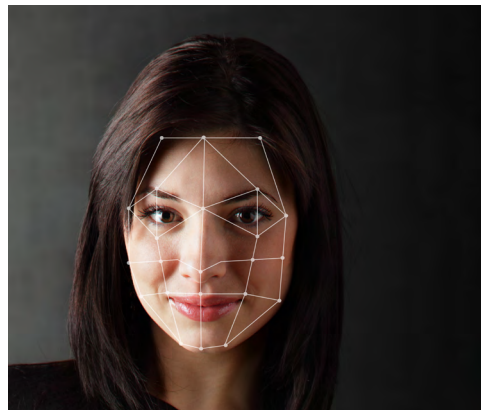
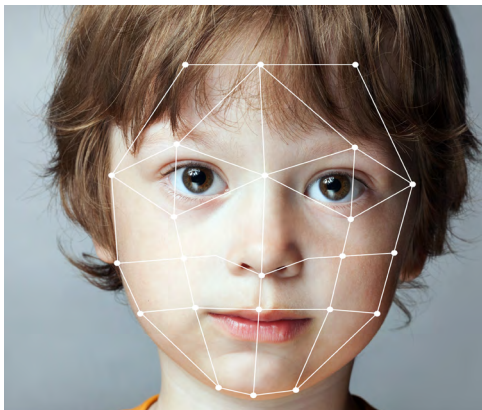
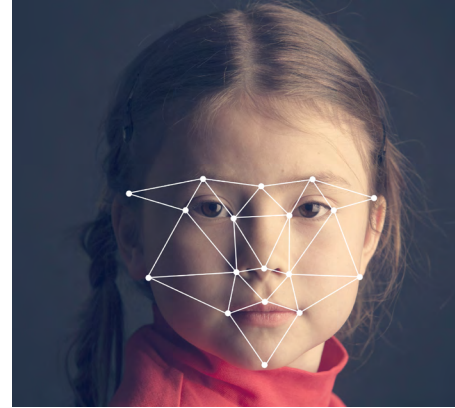
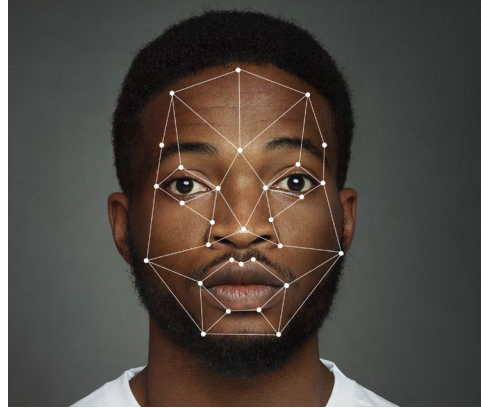
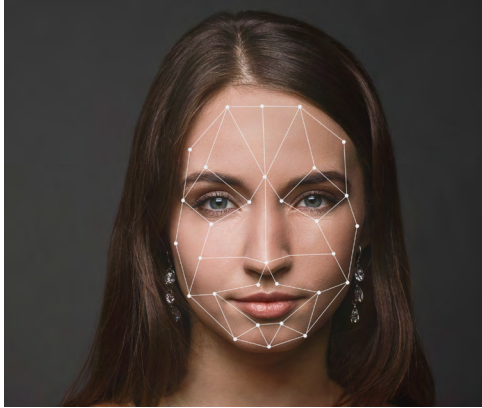
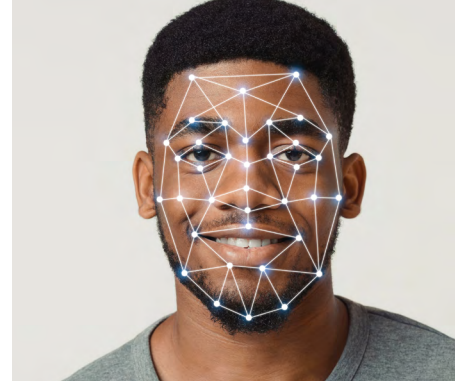
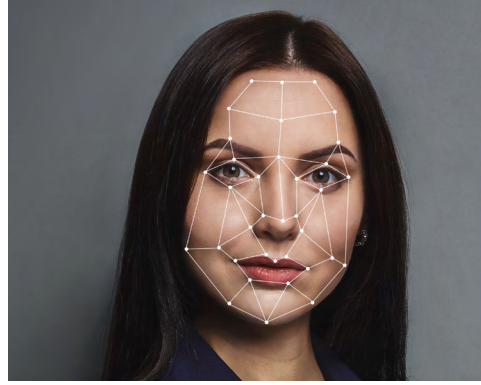
<sup>11</sup> University of Richmond Law Review. Laperruque, Jake. *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*. March 2017. <http://lawreview.richmond.edu/files/2017/03/Laperruque-513-website.pdf>, accessed 8 February, 2021.

<sup>12</sup> [http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live\\_facial\\_recognition\\_final\\_report\\_may\\_2019.pdf](http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf)

<sup>13</sup> Georgetown Law Center on Privacy & Technology. Garvie, Clare; Alvaro Bedorya, and Jonathan Frankle. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. <https://www.perpetualline-up.org/>, accessed 8 February, 2021.

<sup>14</sup> This concept was again used in the Arte TV documentary by Sylvain Louvet called “Tous surveillés, 7 milliards de suspects” (Everyone is being watched, 7 billion suspects). This documentary won the Albert Londres price (highest French Journalism award) for best documentary in 2020.

<sup>15</sup> The Guardian. Naughton, John. *'The goal is to automate us': welcome to the age of surveillance capitalism*. 20 January, 2019. <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook>, accessed 8 February, 2021.



**€140 B**

AUM as of  
31 December 2020



**570**

Experienced and  
committed professionals



**25 years**

Leading the way in  
sustainable investing

**This document is provided for information and educational purposes only and may contain Candriam's opinion and proprietary information.** The opinions, analysis and views expressed in this document are provided for information purposes only, it does not constitute an offer to buy or sell financial instruments, nor does it represent an investment recommendation or confirm any kind of transaction.

Although Candriam selects carefully the data and sources within this document, errors or omissions cannot be excluded a priori. Candriam cannot be held liable for any direct or indirect losses as a result of the use of this document. The intellectual property rights of Candriam must be respected at all times, contents of this document may not be reproduced without prior written approval.

The present document does not constitute investment research as defined by Article 36, paragraph 1 of the Commission delegated regulation (EU) 2017/565. Candriam stresses that this information has not been prepared in compliance with the legal provisions promoting independent investment research, and that it is not subject to any restriction prohibiting the execution of transactions prior to the dissemination of investment research.

This document is not intended to promote and/or offer and/or sell any product or service. The document is also not intended to solicit any request for providing services.