THALES
Building a future we can all trust

Last updated: 24 June 2021- 14 min read.

Face recognition – fascinating and intriguing

Few biometric technologies are sparking our imagination quite like **facial recognition.**

Equally, its arrival prompted profound concerns and surprising reactions in recent years.

But more about that later.

In this web dossier, you will discover the seven face recognition facts and trends that shape the landscape in 2021.

1. Top technologies and providers
2. AI impact - Getting better all the time.
3. 2019-2024 markets and dominant use-cases
4. Face recognition in China, India, the United States, the EU, the UK, Brazil, Russia…
5. Privacy vs security: laissez-faire or freeze, regulate, or ban?
6. Latest hacks: can facial recognition be fooled?
7. Towards hybridized solutions.

Let’s jump right in.

How facial recognition works

Facial recognition is the process of identifying or verifying a person's identity using their face. It captures, analyzes, and compares patterns based on the person's facial details.

1. The **face detection** process is an essential step in detecting and locating human faces in images and videos.
2. The **face capture** process transforms analog information (a face) into digital information (data or vectors) based on the person's facial features.
3. The **face match** process verifies if two faces belong to the same person.

THALES
Building a future we can all trust

A student from the greater Washington DC area used an open-source facial extraction app to detect and deduplicate over 6,000 images of faces from 827 videos posted on Parler during the 6 January event outside and inside the Capitol building (source: Wired 20 January 2021.) He created a website called **Faces of the Riot**, displaying these portraits.

1. Demonstrators, rioters, and journalists have done part of the face capture step with their smartphones (analog face to digital picture).
2. He used facial detection to extract faces from 200K images.
3. It's up to the FBI to investigate, transform the portraits (digital pixels to vectors) and potentially do the face match with existing databases and identify the individuals (with an AFIS / ABIS system).

Today it's considered to be the most natural of all biometric measurements.

And for a good reason – we recognize ourselves not by looking at our fingerprints or irises, for example, but by looking at our faces.

Before we go any further, let's quickly define two keywords: "identification" and "authentication."

Face recognition data to identify and verify

Biometrics are used to identify and authenticate a person using recognizable and verifiable data unique and specific to that person.

For more on biometrics definition, visit our web dossier on biometrics.

Identification answers the question: "Who are you?"

Authentication answers the question: "Are you really who you say you are?"

Stay with us. Here are some examples :

- In the case of facial biometrics, a 2D or 3D sensor "captures" a face. It then transforms it into digital data by applying **an algorithm** before comparing the image captured to those held in a database.

- These automated systems can be used to identify or check an individual's identity in just a few seconds based on their **facial features (geometry)**: spacing of the eyes, bridge of the nose, the contour of the lips, ears, chin, etc.

Of course, other signatures via the human body also exist, such as fingerprints, iris scans, voice recognition, digitization of veins in the palm, and behavioral measurements.

Why face recognition, then?

Facial biometrics continues to be the preferred biometric benchmark.

That's because it's easy to deploy and implement. There is no physical interaction with the end user.

Moreover, face detection and face match processes for verification/identification are speedy.

So, what is the **best face recognition software**?

#1 Top facial recognition technologies

Several projects are vying for the top spot in the race for biometric innovation.

Google, Apple, Facebook, Amazon, and Microsoft (GAFAM) are also very much in the mix.

All the software web giants now regularly publish their theoretical discoveries in artificial intelligence, image recognition, and face analysis to further our understanding as rapidly as possible.

Let's take a closer look :

Academia

The GaussianFace algorithm developed in 2014 by researchers at The Chinese University of Hong Kong achieved facial identification scores of 98.52% compared with the 97.53% achieved by humans. An excellent rating, despite weaknesses regarding memory capacity required and calculation times.

Facebook and Google

In 2014, Facebook announced its **DeepFace** program, which can determine whether two photographed faces belong to the same person, with an accuracy rate of 97.25%. When taking the same test, humans answer correctly in 97.53% of cases, or just 0.28% better than the Facebook program.

THALES
Building a future we can all trust

This technology is incorporated into **Google Photos** and used to sort pictures and automatically tag them based on the people recognized.

Proving its importance in the biometrics landscape, it was quickly followed by the online release of an unofficial open-source version, OpenFace.

Microsoft, IBM, and Megvii

A study done by MIT researchers in February 2018 found that Microsoft, IBM, and China-based Megvii (FACE++) tools had high error rates when identifying darker-skin women compared to lighter-skin men.

At the end of June 2018, Microsoft announced that it had substantially improved its biased facial recognition technology in a blog post.

Amazon

In May 2018, Ars Technica reported that Amazon is already actively promoting its cloud-based face recognition service named, **Rekognition,** to law enforcement agencies. The solution could recognize as many as 100 people in a single image and perform face matches against databases containing tens of millions of faces.

In July 2018, Newsweek reported that Amazon's facial recognition technology falsely identified 28 US Congress members as people arrested for crimes.

Key biometric matching technology providers

At the end of May 2018, the US Homeland Security Science and Technology Directorate published the results of sponsored tests at the Maryland Test Facility (MdTF). These real-life tests measured the performance of **12 face recognition systems** in a corridor measuring 2 m by 2.5 m.

Thales' solution utilizing Facial recognition software (LFIS) achieved excellent results with a face acquisition rate of 99.44% in less than 5 seconds (against an average of 68%), a Vendor True Identification Rate of 98% in less than 5 seconds compared with an average 66%. It also achieved an error rate of 1% compared with an average of 32%.

March 2018 – The live testing using more than 300 volunteers identified the best-performing facial recognition technologies.

More on performance benchmarks: The NIST (National Institute of Standards and Technology) report, published in November 2018, details recognition accuracy for 127 algorithms and associates performance with participant names.

THALES
Building a future we can all trust

FRR: Critics were wrong!

In NIST's reports (August 2020 and March 2021) entitled "Face recognition accuracy with **face masks** using post-COVID-19 algorithms", we see how algorithms are increasing their performance in less than a year.

Facial Emotion Recognition (FER)

Facial Emotion Recognition (from real-time or static images)is the process of mapping facial expressions to identify emotions such as disgust, joy, anger, surprise, fear, or sadness - or compound emotion such as sadness, anger - on a human face with image processing software.

There are also three steps in the recognition or interpretation of human emotions:

- 1) Face detection
- 2) Face expression detection
- 3) Assignment of expression to a specific emotional state.

Facial emotion detection's popularity comes from the vast areas of potential applications.

It's different from facial recognition, which aims to identify a person, not an emotion.

Face expression may be represented by geometric or appearance features, parameters extracted from transformed images such as eigenfaces, dynamic, and 3D models.

Providers include Kairos (face and emotion recognition for brand marketing), Noldus, Affectiva, or Sightcorp.

More on Facial Emotion Recognition (FER) in this May 2021 EU's white paper.

#2 Learning to learn through deep learning

The feature common to all these disruptive technologies is Artificial Intelligence (A.I.) and, more precisely, deep learning, where a system can learn from data.

Why is it important?

It's a **central component** of the latest-generation algorithms developed by Thales and other key players. It holds the secret to face detection, face tracking, face match, and real-time translation of conversations.

The result?

Face recognition systems are getting better all the time.

According to a recent NIST report, massive gains in recognition accuracy have been made in the last five years (2013- 2018) and exceed the 2010-2013 period.

Most of the face recognition algorithms in 2018 outperformed the most accurate algorithm from late 2013.

THALES
Building a future we can all trust

In NIST's 2020 tests, the best facial identification algorithm has an error rate of 0.08% - that's less than one error for 1.000 images. (source: How accurate are facial recognition systems, CSIS)

Yes, you understand that, right?

It's a 50x improvement over six years.

Think about it this way:

Artificial neural network algorithms are helping face recognition algorithms to be more accurate.

How does facial recognition work?

#3 Facial recognition markets

Face recognition markets

A study published in June 2019 estimates that by 2024, the global facial recognition market would generate $7billion of revenue, supported by a compound annual growth rate (CAGR) of 16% over 2019-2024.

For 2019, the market was estimated at $3.2 billion.

The two most significant drivers of this growth are surveillance in the public sector and numerous other applications in diverse market segments.

According to the study, the top **facial recognition vendors include** :

Accenture, Aware, BioID, Certibio, Fujitsu, Fulcrum Biometrics, Thales, HYPR, Idemia, Leidos, M2SYS, NEC, Nuance, Phonexia, and Smilepass.

The main facial recognition applications can be grouped into three principal categories.

THALES
Building a future we can all trust

1. Security - law enforcement

Forensic specialists can use Automated Biometric Identification Systems (ABIS) to compare multiple types of biometrics.

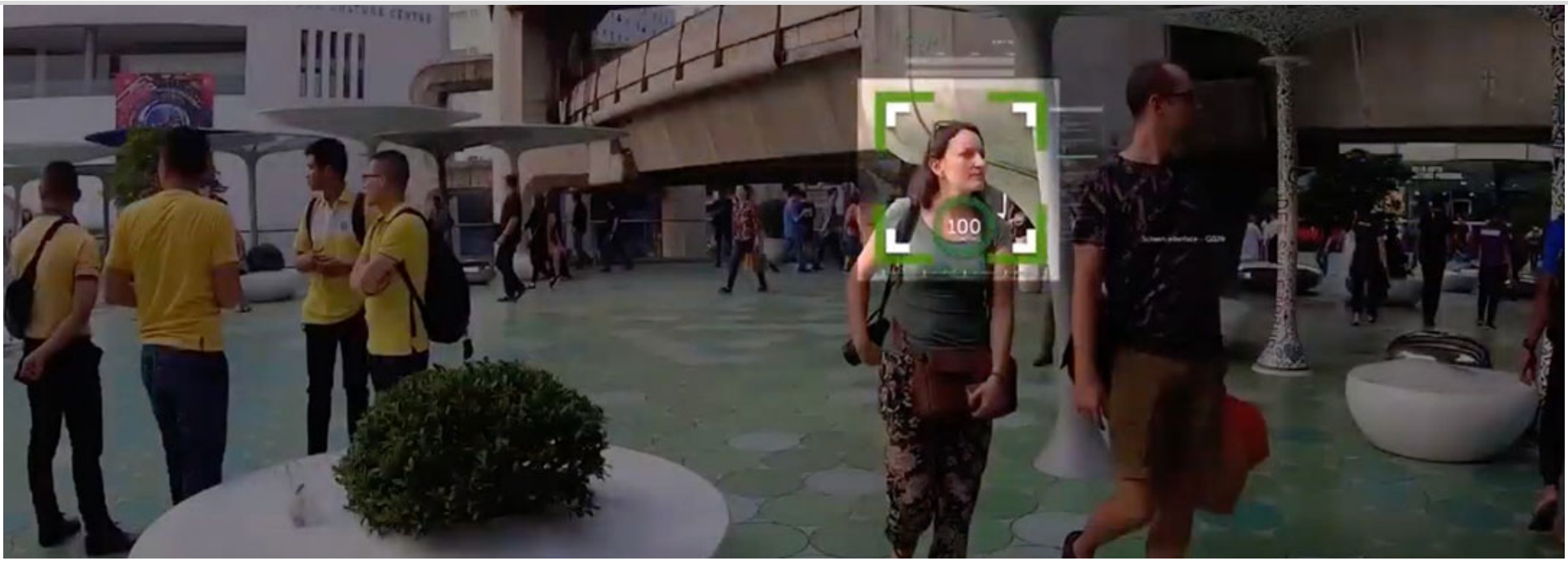
This market is led by increased activity to combat crime and terrorism.

The benefits of facial recognition systems for policing are evident: detection and prevention of crime.

- Facial recognition is used when **issuing identity documents** and, most often, combined with other biometric technologies such as fingerprints (preventing I.D. fraud and identity theft).
- Face match is used at **border checks** to compare the portrait on a digitized biometric passport with the holder's face. In 2017, Thales supplied the new automated control gates for the PARAFE system (Automated Fast Track Crossing at External Borders) at **Roissy Charles de Gaulle Airport in Paris**. This solution has been devised to facilitate the evolution from fingerprint recognition to facial recognition in 2018.
- Face biometrics can also be employed in **police checks**, although it is rigorously controlled in Europe. In 2016, the "man in the hat" responsible for the Brussels terror attacks was identified thanks to FBI facial recognition software. The South Wales Police implemented it at the UEFA Champions League Final 2017.
- In the United States, 26 states (and probably as many as 30) allow law enforcement to run searches against their databases of driver's licenses and I.D. photos. The FBI has access to driver's license photos from 18 states.
- **Drones** and aerial cameras offer an exciting combination of facial recognition applied to large areas during mass events. According to the Keesing Journal of Documents and Identity of June 2018, some hovering drone systems can carry a 10-kilo camera lens that can identify a suspect from 800 meters to a height of 100 meters. The drone can be connected to the ground via a power cable with an unlimited **power supply**. The communication to ground control can't be intercepted as it also uses a line.
- **Facial recognition CCTV systems can** improve performance in carrying out public security missions. Let's illustrate this with four examples:

1. Find missing children and disoriented adults.
2. Identify and find exploited children.
3. Identify and track criminals.
4. Support and accelerate investigations.

THALES
Building a future we can all trust



1. Find Missing children and disoriented adults.

Face recognition CCTV systems can significantly accelerate operators' efforts by enabling them to add a reference photo provided by the missing child's parents and match it with past appearances of that face captured on video. Police can use face recognition to search video sequences (aka **video analytics**) of the estimated location and time the child has been declared missing.

Read more on how Delhi Police used a facial recognition system to trace 3,000 missing children in 4 days.

Police officers can better figure out the child's movements before going missing and locate where he/she was last seen. A real-time alert can trigger an alarm whenever there's a match.Police can then confirm its accuracy and do what's necessary to recover the missing children. The same process can be applied for disoriented **missing adults** (e.g., with dementia, amnesia, epilepsy, or Alzheimer's disease).

THALES
Building a future we can all trust

2. Identify and find exploited children.

Isolating the appearances of specific individuals in a video sequence is critical. It can accelerate investigators' jobs in **child exploitation** cases as well.

Video analytics can help build chronologies, track activity on a map, reveal details, and discover non-obvious connections among the players in a case.

3. Identify and track criminals.

Face recognition CCTV can be used to enable police to track and **identify past criminals** suspected of perpetrating an additional infraction. Police can also take **preventive actions**. By using an image of a known criminal from a video or an external picture (or a database), operators can detect matches in live video and react before it's too late.

4. Support and accelerate investigations.

Facial recognition CCTV systems can be used to support investigators searching for video evidence in the aftermath of an incident.

The ability to isolate suspects and individuals' appearances is critical for accelerating investigators' review of video evidence for relevant details. They can better understand how situations developed.

2. Health

Significant advances have been made in this area.
Thanks to deep learning and face analysis, it is already possible to:

- track a patient's use of medication more accurately
- detect genetic diseases such as DiGeorge syndrome with a success rate of 96.6%
- support pain management procedures.

THALES
Building a future we can all trust

3. Banking and retail

This area is undoubtedly the one where facial recognition was least expected. And yet, quite possibly, it promises the most.

Know Your Customer (KYC) with **facial recognition online** will be a hot topic in 2021.

Why?

Because 64% of primary checking account openings were done online in Q2 2020 (and 36% in branches) in the United States alone.

The pandemic has accelerated this emerging dynamic, and many branches are temporarily closed.

Besides, increased mobile usage urges businesses to focus on mobile-first and develop **fully mobile user-friendly onboarding experiences**.

During the selfie process, the technology shall provide a liveness detection to avoid fraud using a static image.

Liveness detection proves that the selfie taken comes from a live person.

The result?

Adapting to current customer preferences, financial institutions (F.I.s) invest in digital onboarding through online and mobile channels.

THALES
Building a future we can all trust

According to Forbes, digital account opening (DAO) was the most popular technology in banking for the third consecutive year. Nearly 80% of financial institutions add new DAO systems or enhance existing ones in 2020 and 2021.

This important trend is combined with the latest marketing advances in customer experience.

By placing cameras in retail outlets, it is now possible to analyze shoppers' behavior and improve the customer purchase process.

How exactly?

Like the system recently designed by **Facebook**, sales staff are provided with customer information taken from their social media profiles to produce expertly customized responses.

The American department store Saks Fifth Avenue is already using such a system. Amazon Go stores are reportedly using it.

How long before the selfie payment?

Since 2017, KFC, the American king of fried chicken, and Chinese retail and tech giant Alibaba have been testing a face recognition payment solution in Hangzhou, China.

In March 2021, **52 Perekrestok stores** (Перекрёсток) from X5 retail group launched touchless payment by face for self-service checkout terminals with Visa Payment System and Sberbank.

The facial recognition payment system would be used in 3,000 stores by yearend, according to Yahoo!

There's more.

According to Interfax, muscovites can pay for metro rides at the end of 2021.

#4 Mapping of new users

While the United States currently offers the largest market for face recognition opportunities, the **Asia-Pacific region** sees the fastest growth in the sector. China and India lead the field.

Face recognition in China

Face recognition technology is the new hot topic in China, from banks and airports to police.

Now authorities are expanding the facial recognition sunglasses program as police are beginning to use them in Beijing's outskirts.

China is also setting up and perfecting a video surveillance network countrywide.

According to CNBC, over 200 million surveillance cameras were used in 2018; over 500 million are expected by 2021.

The **facial recognition towers** in Chinese cities are emblematic of this move.

This is linked to the **social credit system** the Chinese government is developing.

In the TOP 10 cities with the most street cameras per person, Chongqing, Shenzhen, Shanghai, Tianjin, and Ji'nan lead the pack.

London is #6 and Atlanta #10, according to the Guardian of 2 December 2019.

THALES
Building a future we can all trust

China's ambitions in A.I. (and facial recognition technology) are high. The country aims to become a world leader in A.I. by 2030.

Surprisingly, **China provides strong biometric data protection** against private entities AND increases the government's access to personal information.

This paradox is evidenced by privacy expert Emmanuel Pernot- Leplay's report dated 2 November 2020.

Facial recognition in Asia

Facial recognition will be an important topic for the 2020 Olympic Games in Tokyo (postponed to September 2021).

This technology will automatically identify authorized persons and grant them access, enhancing their experience and safety. It's also being used in Japan for easier mobile banking access.

In Sydney, face recognition is undergoing trials at airports to help move people through security much faster and safer.

In India, the Aadhaar project is the largest biometric database in the world. It already provides a unique digital identity number to 1.29 billion residents as of the end of March 2021.

UIDAI, the authority in charge, announced that **facial authentication** would be launched in a phased roll-out.

It's presently being tested for financial services (October 2020.)

Face authentication will be available as an add-on service in fusion mode and another authentication factor like a fingerprint, Iris, or TOTP.

India could also roll out the world's **most extensive face recognition system** in 2021.

The National Crime Records Bureau (NCRB) has issued an RFP inviting bids to develop a nationwide facial recognition system.

According to the 160-page document, the system will be a centralized web application hosted at the NCRB Data Center in Delhi. It will be available for access to all the police stations.

It will automatically identify people from CCTV videos and images. The Bureau states it will help police catch criminals, find missing people, and identify dead bodies.

Other large projects

The Superior Electoral Court (*Tribunal Superior Eleitoral*) is involved in Brazil's nationwide biometric data collection project. The aim is to create a biometric database and unique I.D. cards, recording the information of 140 million citizens.

In Africa, Gabon, Cameroon, and Burkina Faso have chosen Thales to meet the challenges of biometric identity to identify voters uniquely.

Russia's Central Bank has been deploying a countrywide program since 2017 designed to collect faces, voices, iris scans, and fingerprints.

But the process is progressing very slowly, according to the Biometricupdate website of 13 March 2019.

Moscow claims one of the world's largest networks of 160,000 surveillance cameras by the end of 2019 and is fitted with facial recognition technology for public safety.

The roll-out started in January 2020.

Russian law does not regulate non-consensual face detection and analysis.

THALES
Building a future we can all trust

#5 When face recognition strengthens the legal system

Facial recognition technologies radically affect the ethical and societal challenges data protection poses.

Do these technological feats, worthy of science-fiction novels, genuinely threaten our freedom?

And with it, our anonymity?

E.U. and U.K. biometric data protection

The General Data Protection Regulation (GDPR) provides a rigorous framework for these practices in Europe and the U.K.

Any investigations into a citizen's private life or business travel habits are out of the question, and any such invasions of privacy carry severe penalties.

Applicable from May 2018, the GDPR supports the principle of a harmonized European framework, particularly protecting the right to be forgotten and giving consent through explicit affirmative action.

Yes, you read it well. **There's now one law for 500 million people**.

This directive is bound to have international repercussions.

U.S. biometric data protection landscape

Without a federal law, cities and states are filling the gap.

The State of Washington was the third U.S. state (after Illinois and Texas) to formally protect biometric data through a new law introduced in June 2017.

California was the fourth state as of January 2020.

The California Consumer Privacy Act (CCPA), passed in June 2018 and effective as of 1 January 2020, will severely impact **privacy rights and consumer protection** for residents of California and the whole nation.

The law is frequently presented as a model for a federal data privacy law.

In that sense, **the CCPA can potentially become as consequential as the GDPR**.

In July 2018, Bradford L. Smith, Microsoft's president, compared the face recognition technology to products like highly regulated medicines, and he urged Congress to study it and oversee its use.

In May 2019, U.S. Rep. Alexandria Ocasio-Cortez voiced her "absolute" concerns in a Committee Hearing on facial recognition Technology (Impact on our Civil Rights and Liberties).

A New York State law called the Stop Hacks and Improve Electronic Data Security (SHIELD) became effective on 21 March 2020. It requires implementing a **cybersecurity program and protective measures for N.Y. State residents.**

THALES
Building a future we can all trust

Facial recognition bans (San Francisco, Somerville, Oakland, San Diego, Boston, Portland)

Privacy and civil rights concerns have escalated in the country as face recognition gains traction as a law enforcement tool, and on 6 May 2019, **San Francisco** voted to **ban facial recognition**.

It is the first ban of its kind on the use of face recognition.

The anti-surveillance ordinance signed by San Francisco's Board of Supervisors bars city agencies, including San Francisco PD, from using the technology as of June 2019.

Yes, this includes law enforcement.

There's more.

As reported by the Boston Globe on 27 June 2019, the Somerville City Council (Massachusetts) voted to ban facial recognition, making the city the second community to make such a decision.

Lather, rinse, repeat.

- On 16 July 2019, **Oakland** (California) took the same decision and became the third U.S. city to ban face recognition technology. It is interesting to note that the Oakland Police Department is not using this technology and was not planning to use it.
- **San Diego** took the same decision at the end of December 2019 before the new Californian law. This new law (Assembly Bill 215) about facial recognition and other biometric surveillance) specifically prohibits the use of police body cameras in California. The ban is in place for three years as of 1 January 2020.
- On 24 June 2020, **Boston** voted to ban face surveillance technology by police, as reported by the Boston Herald.
- **Portland** (Oregon) decided its ban on 9 September 2020 (effective 1 January 2021.) The city is the first to extend it to "private entities in places of public accommodation", such as private stores. (CNN).
- **Massachusetts** passed a reform bill in December 2020 restricting the use of facial recognition. It's applicable as of May 2021.
- **Virginia** legislature passed (April 2021) a new bill (H.B. 2031) that prohibits law enforcement agencies from continuing to use facial recognition software after 1 July 2021.

Since the San Francisco, Sommerville, Oakland, and now San Diego, Boston, and Portland rulings, the debate has gotten louder in many cities and states, not just in the U.S.

In Europe, at the end of August 2019, Sweden's Data Protection Authority decided to ban facial recognition technology in schools. It fined a local high school (the first GDPR penalty in the country).

How to better regulate emerging technologies?

So,

- Should other cities or countries follow this example?
- Is the ban just a "pause button" to better assess risks?
- Is this a step backwards for public safety?
- Is there a policy vacuum? At which level?

Stay tuned for the outcome of all these discussions as the **U.S. Congress** is getting pressure from activists **to ban** the technology and from providers) **to regulate**.

THALES
Building a future we can all trust

has pledged to publish an A.I. legislation blueprint very soon.

The final version of the European Commission whitepaper is available online. The European Commission presented tough draft rules in April 2021. But according to Reuters, it could take years before the regulations come into force.

Similarly, in June 2021, the E.U.'s two privacy watchdogs (EDPB and EDPS) called for a ban on facial recognition in publicly accessible spaces.

Again the questions of privacy, consent, and function creep (data collected for one purpose being used for another)are central to the debate.

In our biometric data dossier, find more on biometric data protection laws(E.U., U.K., and U.S. perspectives).

India and its national biometric identification scheme, Aadhaar

In India, thanks to the Puttaswamy judgment delivered on 27 August 2017, the Supreme Court has enshrined the **right to privacy** in the country's constitution. This decision has rebalanced the relationship between citizens and the state and posed a new challenge to expanding the Aadhaar project.

The Indian government, however, approved the use of the country's biometric EID program by private entities on 28 February 2019.

Rebound effect: the legal system and its professions get even stronger.

As ambassadors and guardians of data protection regulation, data protection officers have become necessary for businesses and have a much sought-after role.

#6 The rebels – facial recognition hackers

Despite this technical and legal arsenal designed to protect data, citizens, and their **anonymity**, critical voices have still been raised.

Some parties are concerned and alarmed by these developments. Some have taken action.

But can facial recognition be fooled?

- Grigory Bakunov in Russia has invented a solution to escape proper face detection and **confuse face detection devices**. He has developed an algorithm that creates special makeup to fool the software. However, he has not brought his product to market after realizing how easily criminals could use it.

THALES
Building a future we can all trust

- In late 2017, a Vietnamese company successfully used a **mask to hack** the Face ID face recognition function of Apple's iPhone X. However, the hack is too complicated to implement for large-scale exploitation.

- Around the same time, researchers from a German company revealed a hack that allowed them to bypass the facial authentication of Windows 10 Hello by printing a f**acial image in infrared**.

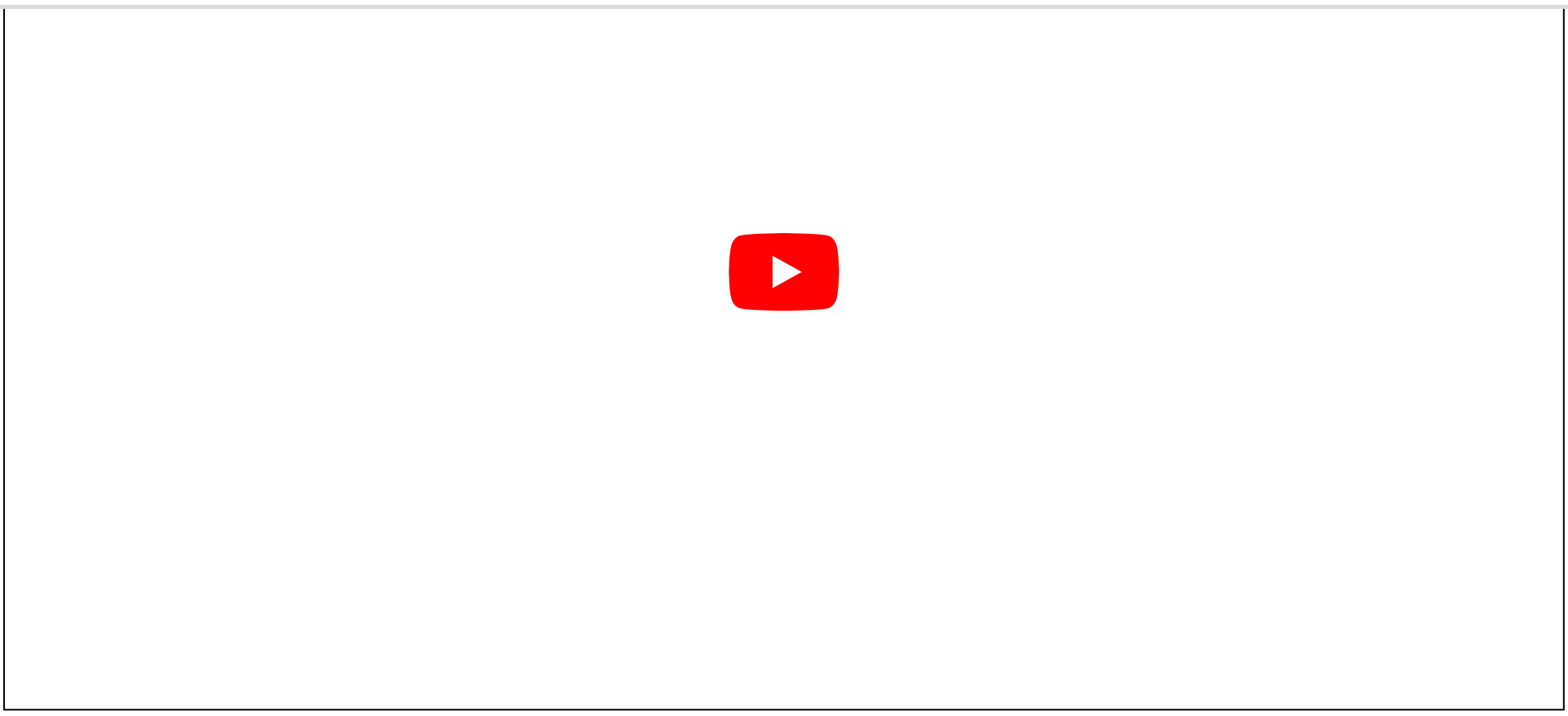
- Forbes announced in May 2018 that researchers from the University of Toronto had developed an **algorithm to disrupt facial recognition** software (aka privacy filter).

- In August 2020, the Verge detailed a "cloaking" app named Fawkes. The software gradually distorts your selfies and other pics you may leave on social media. The tool comes from the University of Chicago's Sand Lab.

In short, a user could apply a filter that modifies specific pixels in an image before putting it on the web. These changes are imperceptible to the human eye but are very confusing for facial recognition algorithms.

- In November 2020, a tool named Anonymizer was made available by Generated Media. The software creates a series of **synthetic portraits** from a picture you can upload. According to the website, the images are mathematically similar to your face and look like you but will trick facial recognition software. It could be an interesting solution to fool systems like Clearview A.I. that are scrapping millions of faces from social media (learn more on the Clearview A.I. controversy).

We tested Anonymizer on 27 November 2020. But the 40+ doppelgangers we got were **far from looking like the original portrait uploaded**.



An interesting experiment by Thomas Smith, published on 28 January 2021, revealed a simple technique to make you invisible.

According to his tests, **wearing a disposable mask and opaque sunglasses** is a powerful combination to render you invisible.

Why?

In that case, the F.R. systems are denied too much valuable information (mouth, nose, eyes, eyebrows) to make a precise facial comparison.

The industry is working on **anti-spoofing mechanisms,** and standardization groups have specifically identified two topics:

1. Make sure the captured image has been done from a person and not from a photograph (2D), a video screen (2D), or a mask (3D) (liveness check or liveness detection)
2. Ensure that two or more individuals' facial images (**morphed portraits**) have not been joined into a reference document, such as a passport.

#7 Further together – towards hybridized solutions

Future identification and authentication solutions will borrow from all aspects of biometrics.

This will lead to a **biometric mix** capable of guaranteeing total security and privacy for all stakeholders in the ecosystem.

It's very much the spirit of Thales Gemalto IdCloud Fraud Prevention, a risk assessment and fraud detection software for payments.

In this solution, **geolocation**, I.P. addresses (the device being used), and **keying patterns** can create a solid combination to authenticate users for online banking or egovernment services securely.

This seventh trend belongs to us.

It's our job to envisage it together and make it happen through high-added-value biometric projects.

> Thales has specialized in biometric technologies for almost 30 years. The company has always collaborated with the best research, ethics, and biometric application players.

THALES
Building a future we can all trust

The months hold many changes in store.

Indeed, we can't claim to predict all the essential topics that will emerge in the short-term future.

Can you fill in some of the gaps?

If you've something to say on facial recognition, tech, trends, a question to ask, or have found this article useful, please leave a comment in the box below.

We'd also welcome any suggestions on how it could be improved or proposals for future articles.

We look forward to hearing from you.

Choosing the right facial recognition solution for access control

Whitepaper

Download the whitepaper

Thales Statement Paper Facial Recognition (Oct 2021)

Thales addresses the main concerns around facial recognition, and highlights our vision for the ethical, socially accountable use of the technology.

Facial Recognition Statement Paper

THALES
Building a future we can all trust

Gemalto exceeds expectations at 2018 Biometric Technology Rally

The Live Face Identification System helps you improve security & efficiency where you need it most. The solution utilizing live facial recognition performed exceptionally well at the rally.

Read the Biometric Technology Rally

12 Jun 2023

Thales TrUE Technology: responsible biometrics

The Thales TrUE Technology approach aims to deliver responsible products and services that build trust for both users and service providers, which is the key to building a safer, greener and more inclusive society.

09 Nov 2021

Thales, the trusted provider of accurate and efficient biometric technologies

Fully adapted to the current Covid context, Thales provides highly accurate biometric authentication and identification methods for smooth and secure user experiences. Thales solutions offer full compliance with GDPR and support ‘touch less’ use cases such as access ma…

Facial recognition
Biometric data protection
Biometric questions
AFIS history
New trends in biometrics
Eagle II Program

Case studies
Get Inspired: Biometrics
Biometrics articles

THALES
Building a future we can all trust

> LiveScan Software
- LiveScan 5.0 Software
> Mobile ID Application
> WebID
> ACE-V Manager

Biometric software
> CABIS
- CABIS 7.0
> Facial Recognition Platform
> LiveScan Software
- LiveScan 5.0 Software
> Mobile ID Application
> WebID
> ACE-V Manager

Biometric Scanners
> Fingerprint Scanners
- Cogent Single Finger Scanner DactyID20
- Cogent DactyScan40p Scanner
- Cogent DactyScan84c Scanner
- Cogent Palm Scanner MultiScan527
- Cogent Palm Scanner MultiScan527g
- Cogent Palm Scanner CS500q

Get in touch with us

For more information regarding our services and solutions contact one of our sales representatives. We have agents worldwide that are available to help with your digital security needs. Fill out our contact form and one of our representatives will be in touch to discuss how we can assist you.
Please note we do not sell any products nor offer support directly to end users. If you have questions regarding one of our products provided by e.g. your bank or government, then please contact them for advice first.

Building a future

DEFENCE AND SECURITY

THALES
Building a future we can all trust

TRANSVERSE MARKETS

SPECIFIC SOLUTIONS

Social networks

Contact us

Thales Headquarters
+33 (0) 1 57 77 80 00

Send a message

GLOBAL

MARKETS

CAREER

INVESTOR

JOURNALIST

CUSTOMER ONLINE

SUPPLIER

 Credits Terms of Use Personal Data Sitemap Accessibility: partially accessible