

# Facial recognition system

A **facial recognition system** is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image.

Development began on similar systems in the 1960s, beginning as a form of computer application. Since their inception, facial recognition systems have seen wider uses in recent times on smartphones and in other forms of technology, such as robotics. Because computerized facial recognition involves the measurement of a human's physiological characteristics, facial recognition systems are categorized as biometrics. Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless process.<sup>[1]</sup> Facial recognition systems have been deployed in advanced human–computer interaction, video surveillance and automatic indexing of images.<sup>[2]</sup>

Facial recognition systems are employed throughout the world today by governments and private companies.<sup>[3]</sup> Their effectiveness varies, and some systems have previously been scrapped because of their ineffectiveness. The use of facial recognition systems has also raised controversy, with claims that the systems violate citizens' privacy, commonly make incorrect identifications, encourage gender norms and racial profiling, and do not protect important biometric data. These claims have led to the ban of facial recognition systems in several cities in the United States.<sup>[4]</sup> As a result of growing societal concerns, Meta announced<sup>[5]</sup> that it plans to shut down Facebook facial recognition system, deleting the face scan data of more than one billion users.<sup>[6]</sup> This change will represent one of the largest shifts in facial recognition usage in the technology's history.



Automatic ticket gate with face recognition system in Osaka Metro Morinomiya Station

## Contents

### History of facial recognition technology

### Techniques for face recognition

Traditional

Human identification at a distance (HID)

3-dimensional recognition

Thermal cameras

### Application

Social media

ID verification

Face ID

Deployment of FRT for availing government services

India

Deployment in security services

[Commonwealth](#)[United States](#)[China](#)[India](#)[Latin America](#)[European Union](#)[Greece](#)[Italy](#)[The Netherlands](#)[South Africa](#)[Deployment in retail stores](#)[United States](#)[Additional uses](#)**[Advantages and disadvantages](#)**[Compared to other biometric systems](#)[Weaknesses](#)[Ineffectiveness](#)**[Controversies](#)**[Privacy violations](#)[Imperfect technology in law enforcement](#)[Data protection](#)**[Bans on the use of facial recognition technology](#)****[Emotion recognition](#)****[Anti-facial recognition systems](#)****[See also](#)****[References](#)****[Further reading](#)****[External links](#)**

## History of facial recognition technology

---

Automated facial recognition was pioneered in the 1960s. [Woody Bledsoe](#), [Helen Chan Wolf](#), and [Charles Bisson](#) worked on using the computer to recognize human faces. Their early facial recognition project was dubbed "man-machine" because the coordinates of the facial features in a photograph had to be established by a human before they could be used by the computer for recognition. On a [graphics tablet](#) a human had to pinpoint the coordinates of facial features such as the pupil centers, the inside and outside corner of eyes, and the [widows peak](#) in the hairline. The coordinates were used to calculate 20 distances, including the width of the mouth and of the eyes. A human could process about 40 pictures an hour in this manner and so build a database of the computed distances. A computer would then automatically compare the distances for each photograph, calculate the difference between the distances and return the closed records as a possible match.<sup>[7]</sup>

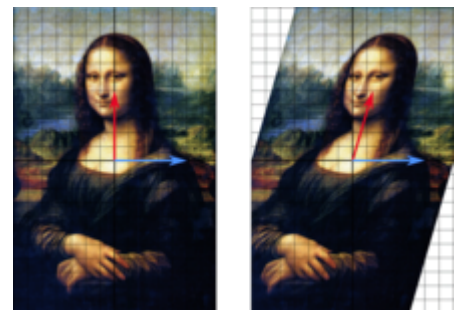
In 1970, [Takeo Kanade](#) publicly demonstrated a face matching system that located anatomical features such as the chin and calculated the distance ratio between facial features without human intervention. Later tests revealed that the system could not always reliably identify facial features. Nonetheless, interest in the subject grew and in 1977 Kanade published the first detailed book on facial recognition technology.<sup>[8]</sup>

In 1993, the Defense Advanced Research Project Agency (DARPA) and the Army Research Laboratory (ARL) established the face recognition technology program FERET to develop "automatic face recognition capabilities" that could be employed in a productive real life environment "to assist security, intelligence, and law enforcement personnel in the performance of their duties." Face recognition systems that had been trialed in research labs were evaluated and the FERET tests found that while the performance of existing automated facial recognition systems varied, a handful of existing methods could viably be used to recognize faces in still images taken in a controlled environment.<sup>[9]</sup> The FERET tests spawned three US companies that sold automated facial recognition systems. Vision Corporation and Miroso Inc were both founded in 1994, by researchers who used the results of the FERET tests as a selling point. Viisage Technology was established by a identification card defense contractor in 1996 to commercially exploit the rights to the facial recognition algorithm developed by Alex Pentland at MIT.<sup>[10]</sup>

Following the 1993 FERET face recognition vendor test the Department of Motor Vehicles (DMV) offices in West Virginia and New Mexico were the first DMV offices to use automated facial recognition systems as a way to prevent and detect people obtaining multiple driving licenses under different names. Driver's licenses in the United States were at that point a commonly accepted form of photo identification. DMV offices across the United States were undergoing a technological upgrade and were in the process of establishing databases of digital ID photographs. This enabled DMV offices to deploy the facial recognition systems on the market to search photographs for new driving licenses against the existing DMV database.<sup>[11]</sup> DMV offices became one of the first major markets for automated facial recognition technology and introduced US citizens to facial recognition as a standard method of identification.<sup>[12]</sup> The increase of the US prison population in the 1990s prompted U.S. states to established connected and automated identification systems that incorporated digital biometric databases, in some instances this included facial recognition. In 1999 Minnesota incorporated the facial recognition system FaceIT by Visionics into a mug shot booking system that allowed police, judges and court officers to track criminals across the state.<sup>[13]</sup>

Until the 1990s facial recognition systems were developed primarily by using photographic portraits of human faces. Research on face recognition to reliably locate a face in an image that contains other objects gained traction in the early 1990s with the principle component analysis (PCA). The PCA method of face detection is also known as Eigenface and was developed by Matthew Turk and Alex Pentland.<sup>[14]</sup> Turk and Pentland combined the conceptual approach of the Karhunen–Loève theorem and factor analysis, to develop a linear model. Eigenfaces are determined based on global and orthogonal features in human faces. A human face is calculated as a weighted combination of a number of Eigenfaces. Because few Eigenfaces were used to encode human faces of a given population, Turk and Pentland's PCA face detection method greatly reduced the amount of data that had to be processed to detect a face. Pentland in 1994 defined Eigenface features, including eigen eyes, eigen mouths and eigen noses, to advance the use of PCA in facial recognition. In 1997 the PCA Eigenface method of face recognition<sup>[15]</sup> was improved upon using linear discriminant analysis (LDA) to produce Fisherfaces.<sup>[16]</sup> LDA Fisherfaces became dominantly used in PCA feature based face recognition. While Eigenfaces were also used for face reconstruction. In these approaches no global structure of the face is calculated which links the facial features or parts.<sup>[17]</sup>

Purely feature based approaches to facial recognition were overtaken in the late 1990s by the Bochum system, which used Gabor filter to record the face features and computed a grid of the face structure to link the features.<sup>[18]</sup> Christoph von der Malsburg and his research team at the University of Bochum



In this shear mapping the red arrow changes direction, but the blue arrow does not and is used as eigenvector.



The Viola–Jones algorithm for face detection uses Haar-like features to locate faces in an image. Here a Haar Feature that looks similar to the bridge of the nose is applied onto the face.

developed Elastic Bunch Graph Matching in the mid 1990s to extract a face out of an image using skin segmentation.<sup>[19]</sup> By 1997 the face detection method developed by Malsburg outperformed most other facial detection systems on the market. The so-called "Bochum system" of face detection was sold commercially on the market as ZN-Face to operators of airports and other busy locations. The software was "robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hairstyles and glasses—even sunglasses".<sup>[20]</sup>

Real-time face detection in video footage became possible in 2001 with the Viola–Jones object detection framework for faces.<sup>[21]</sup> Paul Viola and Michael Jones combined their face detection method with the Haar-like feature approach to object recognition in digital images to launch AdaBoost, the first real-time frontal-view face detector.<sup>[22]</sup> By 2015 the Viola-Jones algorithm had been implemented using small low power detectors on handheld devices and embedded systems. Therefore, the Viola-Jones algorithm has not only broadened the practical application of face recognition systems but has also been used to support new features in user interfaces and teleconferencing.<sup>[23]</sup>

## Techniques for face recognition

While humans can recognize faces without much effort,<sup>[24]</sup> facial recognition is a challenging pattern recognition problem in computing. Facial recognition systems attempt to identify a human face, which is three-dimensional and changes in appearance with lighting and facial expression, based on its two-dimensional image. To accomplish this computational task, facial recognition systems perform four steps. First face detection is used to segment the face from the image background. In the second step the segmented face image is aligned to account for face pose, image size and photographic properties, such as illumination and grayscale. The purpose of the alignment process is to enable the accurate localization of facial features in the third step, the facial feature extraction. Features such as eyes, nose and mouth are pinpointed and measured in the image to represent the face. The so established feature vector of the face is then, in the fourth step, matched against a database of faces.<sup>[25]</sup>

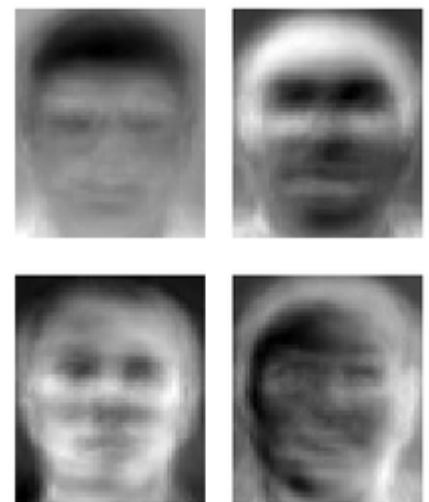


Automatic face detection with OpenCV.

### Traditional

Some face recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw.<sup>[26]</sup> These features are then used to search for other images with matching features.<sup>[27]</sup>

Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data.<sup>[28]</sup> One of the earliest successful systems<sup>[29]</sup> is based on template matching techniques<sup>[30]</sup> applied to a set of salient facial features, providing a sort of compressed face representation.



Some eigenfaces from AT&T Laboratories Cambridge

Recognition algorithms can be divided into two main approaches: geometric, which looks at distinguishing features, or photo-metric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances. Some

classify these algorithms into two broad categories: holistic and feature-based models. The former attempts to recognize the face in its entirety while the feature-based subdivide into components such as according to features and analyze each as well as its spatial location with respect to other features.<sup>[31]</sup>

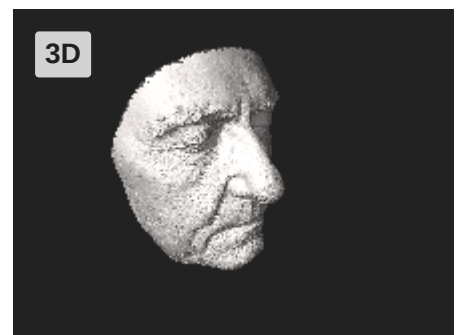
Popular recognition algorithms include principal component analysis using eigenfaces, linear discriminant analysis, elastic bunch graph matching using the Fisherface algorithm, the hidden Markov model, the multilinear subspace learning using tensor representation, and the neuronal motivated dynamic link matching.<sup>[32]</sup> Modern facial recognition systems make increasing use of machine learning techniques such as deep learning<sup>[33]</sup>

## Human identification at a distance (HID)

To enable human identification at a distance (HID) low-resolution images of faces are enhanced using face hallucination. In CCTV imagery faces are often very small. But because facial recognition algorithms that identify and plot facial features require high resolution images, resolution enhancement techniques have been developed to enable facial recognition systems to work with imagery that has been captured in environments with a high signal-to-noise ratio. Face hallucination algorithms that are applied to images prior to those images being submitted to the facial recognition system use example-based machine learning with pixel substitution or nearest neighbour distribution indexes that may also incorporate demographic and age related facial characteristics. Use of face hallucination techniques improves the performance of high resolution facial recognition algorithms and may be used to overcome the inherent limitations of super-resolution algorithms. Face hallucination techniques are also used to pre-treat imagery where faces are disguised. Here the disguise, such as sunglasses, is removed and the face hallucination algorithm is applied to the image. Such face hallucination algorithms need to be trained on similar face images with and without disguise. To fill in the area uncovered by removing the disguise, face hallucination algorithms need to correctly map the entire state of the face, which may be not possible due to the momentary facial expression captured in the low resolution image.<sup>[34]</sup>

## 3-dimensional recognition

Three-dimensional face recognition technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin.<sup>[35]</sup> One advantage of 3D face recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view.<sup>[35][27]</sup> Three-dimensional data points from a face vastly improve the precision of face recognition. 3D-dimensional face recognition research is enabled by the development of sophisticated sensors that project structured light onto the face.<sup>[36]</sup> 3D matching technique are sensitive to expressions, therefore researchers at Technion applied tools from metric geometry to treat expressions as isometries.<sup>[37]</sup> A new method of capturing 3D images of faces uses three tracking cameras that point at different angles; one camera will be pointing at the front of the subject, second one to the side, and third one at an angle. All these cameras will work together so it can track a subject's face in real-time and be able to face detect and recognize.<sup>[38]</sup>



3D model of a human face.

## Thermal cameras



A different form of taking input data for face recognition is by using thermal cameras, by this procedure the cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or makeup.<sup>[39]</sup> Unlike conventional cameras, thermal cameras can capture facial imagery even in low-light and nighttime conditions without using a flash and exposing the position of the camera.<sup>[40]</sup> However, the databases for face recognition are limited. Efforts to build databases of thermal face images date back to 2004.<sup>[39]</sup> By 2016 several databases existed, including the IIITD-PSE and the Notre Dame thermal face database.<sup>[41]</sup> Current thermal face recognition systems are not able to reliably detect a face in a thermal image that has been taken of an outdoor environment.<sup>[42]</sup>



A pseudocolor image of two people taken in long-wavelength infrared (body-temperature thermal) light.

In 2018, researchers from the U.S. Army Research Laboratory (ARL) developed a technique that would allow them to match facial imagery obtained using a thermal camera with those in databases that were captured using a conventional camera.<sup>[43]</sup> Known as a cross-spectrum synthesis method due to how it bridges facial recognition from two different imaging modalities, this method synthesizes a single image by analyzing multiple facial regions and details.<sup>[44]</sup> It consists of a non-linear regression model that maps a specific thermal image into a corresponding visible facial image and an optimization issue that projects the latent projection back into the image space.<sup>[40]</sup> ARL scientists have noted that the approach works by combining global information (i.e. features across the entire face) with local information (i.e. features regarding the eyes, nose, and mouth).<sup>[45]</sup> According to performance tests conducted at ARL, the multi-region cross-spectrum synthesis model demonstrated a performance improvement of about 30% over baseline methods and about 5% over state-of-the-art methods.<sup>[44]</sup>

## Application

### Social media

Founded in 2013, Looksery went on to raise money for its face modification app on Kickstarter. After successful crowdfunding, Looksery launched in October 2014. The application allows video chat with others through a special filter for faces that modifies the look of users. Image augmenting applications already on the market, such as Facetune and Perfect365, were limited to static images, whereas Lookser'y allowed augmented reality to live videos. In late 2015 SnapChat purchased Lookser'y, which would then become its landmark lenses function.<sup>[46]</sup> Snapchat filter applications use face detection technology and on the basis of the facial features identified in an image a 3D mesh mask is layered over the face.<sup>[47]</sup>

DeepFace is a deep learning facial recognition system created by a research group at Facebook. It identifies human faces in digital images. It employs a nine-layer neural net with over 120 million connection weights, and was trained on four million images uploaded by Facebook users.<sup>[48][49]</sup> The system is said to be 97% accurate, compared to 85% for the FBI's Next Generation Identification system.<sup>[50]</sup>

TikTok's algorithm has been regarded as especially effective, but many were left to wonder at the exact programming that caused the app to be so effective in guessing the user's desired content.<sup>[51]</sup> In June 2020, TikTok released a statement regarding the "For You" page, and how they recommended videos to users, which did not include facial recognition.<sup>[52]</sup> In February 2021, however, TikTok agreed to a \$92 million settlement to a US lawsuit which alleged that the app had used facial recognition in both user videos and its algorithm to identify age, gender and ethnicity.<sup>[53]</sup>

### ID verification

The emerging use of facial recognition is in the use of ID verification services. Many companies and others are working in the market now to provide these services to banks, ICOs, and other e-businesses.<sup>[54]</sup> Face recognition has been leveraged as a form of biometric authentication for various computing platforms and devices;<sup>[27]</sup> Android 4.0 "Ice Cream Sandwich" added facial recognition using a smartphone's front camera as a means of unlocking devices,<sup>[55][56]</sup> while Microsoft introduced face recognition login to its Xbox 360 video game console through its Kinect accessory,<sup>[57]</sup> as well as Windows 10 via its "Windows Hello" platform (which requires an infrared-illuminated camera).<sup>[58]</sup> In 2017 Apple's iPhone X smartphone introduced facial recognition to the product line with its "Face ID" platform, which uses an infrared illumination system.<sup>[59]</sup>

## Face ID

Apple introduced Face ID on the flagship iPhone X as a biometric authentication successor to the Touch ID, a fingerprint based system. Face ID has a facial recognition sensor that consists of two parts: a "Romeo" module that projects more than 30,000 infrared dots onto the user's face, and a "Juliet" module that reads the pattern.<sup>[60]</sup> The pattern is sent to a local "Secure Enclave" in the device's central processing unit (CPU) to confirm a match with the phone owner's face.<sup>[61]</sup>

The facial pattern is not accessible by Apple. The system will not work with eyes closed, in an effort to prevent unauthorized access.<sup>[61]</sup> The technology learns from changes in a user's appearance, and therefore works with hats, scarves, glasses, and many sunglasses, beard and makeup.<sup>[62]</sup> It also works in the dark. This is done by using a "Flood Illuminator", which is a dedicated infrared flash that throws out invisible infrared light onto the user's face to properly read the 30,000 facial points.<sup>[63]</sup>

## Deployment of FRT for availing government services

### India

In an interview, the National Health Authority chief Dr. R.S. Sharma said that facial recognition technology would be used in conjunction with Aadhaar to authenticate the identity of people seeking vaccines.<sup>[64]</sup> Ten human rights and digital rights organizations and more than 150 individuals signed a statement by the Internet Freedom Foundation that raised alarm against the deployment of facial recognition technology in the central government's vaccination drive process.<sup>[65]</sup> Implementation of an error-prone system without adequate legislation containing mandatory safeguards, would deprive citizens of essential services and linking this untested technology to the vaccination roll-out in India will only exclude persons from the vaccine delivery system.<sup>[66]</sup>

In July, 2021, a press release by the Government of Meghalaya stated that facial recognition technology (FRT) would be used to verify the identity of pensioners to issue a Digital Life Certificate using "Pensioner's Life Certification Verification" mobile application.<sup>[67]</sup> The notice, according to the press release, purports to offer pensioners "a secure, easy and hassle-free interface for verifying their liveness to the Pension Disbursing Authorities from the comfort of their homes using smart phones". Mr. Jade Jeremiah Lyngdoh, a law student, sent a legal notice to the relevant authorities highlighting that "The application has been rolled out without any anchoring legislation which governs the processing of personal data and thus, lacks lawfulness and the Government is not empowered to process data."<sup>[68]</sup>

## Deployment in security services

### Commonwealth

The Australian Border Force and New Zealand Customs Service have set up an automated border processing system called SmartGate that uses face recognition, which compares the face of the traveller with the data in the e-passport microchip.<sup>[69][70]</sup> All Canadian international airports use facial recognition as part of the Primary Inspection Kiosk program that compares a traveler face to their photo stored on the ePassport. This program first came to Vancouver International Airport in early 2017 and was rolled up to all remaining international airports in 2018–2019.<sup>[71]</sup>



Swiss European surveillance: face recognition and vehicle make, model, color and license plate reader

Police forces in the United Kingdom have been trialing live facial recognition technology at public events since 2015.<sup>[72]</sup> In May 2017, a man was arrested using an automatic facial recognition (AFR) system mounted on a van operated by the South Wales Police. Ars Technica reported that "this appears to be the first time [AFR] has led to an arrest".<sup>[73]</sup> However, a 2018 report by Big Brother Watch found that these systems were up to 98% inaccurate.<sup>[72]</sup> The report also revealed that two UK police forces, South Wales Police and the Metropolitan Police, were using live facial recognition at public events and in public spaces.<sup>[74]</sup> In September 2019, South Wales Police use of facial recognition was ruled lawful.<sup>[74]</sup> Live facial recognition has been trialled since 2016 in the streets of London and will be used on a regular basis from Metropolitan Police from beginning of 2020.<sup>[75]</sup> In August 2020 the Court of Appeal ruled that the way the facial recognition system had been used by the South Wales Police in 2017 and 2018 violated human rights.<sup>[76]</sup>

## United States

The U.S. Department of State operates one of the largest face recognition systems in the world with a database of 117 million American adults, with photos typically drawn from driver's license photos.<sup>[77]</sup> Although it is still far from completion, it is being put to use in certain cities to give clues as to who was in the photo. The FBI uses the photos as an investigative tool, not for positive identification.<sup>[78]</sup> As of 2016, facial recognition was being used to identify people in photos taken by police in San Diego and Los Angeles (not on real-time video, and only against booking photos)<sup>[79]</sup> and use was planned in West Virginia and Dallas.<sup>[80]</sup>



Flight boarding gate with "biometric face scanners" developed by U.S. Customs and Border Protection at Hartsfield–Jackson Atlanta International Airport.

In recent years Maryland has used face recognition by comparing people's faces to their driver's license photos. The system drew controversy when it was used in Baltimore to arrest unruly protesters after the death of Freddie Gray in police custody.<sup>[81]</sup> Many other states are using or developing a similar system however some states have laws prohibiting its use.

The FBI has also instituted its Next Generation Identification program to include face recognition, as well as more traditional biometrics like fingerprints and iris scans, which can pull from both criminal and civil databases.<sup>[82]</sup> The federal General Accountability Office criticized the FBI for not addressing various concerns related to privacy and accuracy.<sup>[83]</sup>

Starting in 2018, U.S. Customs and Border Protection deployed "biometric face scanners" at U.S. airports. Passengers taking outbound international flights can complete the check-in, security and the boarding process after getting facial images captured and verified by matching their ID photos stored on CBP's database. Images captured for travelers with U.S. citizenship will be deleted within up to 12-hours. TSA had



expressed its intention to adopt a similar program for domestic air travel during the security check process in the future. The American Civil Liberties Union is one of the organizations against the program, concerning that the program will be used for surveillance purposes.<sup>[84]</sup>

In 2019, researchers reported that Immigration and Customs Enforcement uses facial recognition software against state driver's license databases, including for some states that provide licenses to undocumented immigrants.<sup>[83]</sup>

## China

In 2006, the Skynet Project was initiated by the Chinese Government to implement CCTV surveillance nationwide and as of 2018, there has been 20 million cameras, many of which capable of real-time facial recognition, deployed across the country for this project<sup>[85]</sup> Some official claim that the current Skynet system can scan the entire Chinese population in one second and the world population in two seconds.<sup>[86]</sup>

In 2017 the Qingdao police was able to identify twenty-five wanted suspects using facial recognition equipment at the Qingdao International Beer Festival, one of which had been on the run for 10 years.<sup>[87]</sup> The equipment works by recording a 15-second video clip and taking multiple snapshots of the subject. That data is compared and analyzed with images from the police department's database and within 20 minutes, the subject can be identified with a 98.1% accuracy.<sup>[88]</sup>

In 2018, Chinese police in Zhengzhou and Beijing were using smart glasses to take photos which are compared against a government database using facial recognition to identify suspects, retrieve an address, and track people moving beyond their home areas.<sup>[89][90]</sup>



Boarding gates with facial recognition technology at Beijing West railway station

As of late 2017, China has deployed facial recognition and artificial intelligence technology in Xinjiang. Reporters visiting the region found surveillance cameras installed every hundred meters or so in several cities, as well as facial recognition checkpoints at areas like gas stations, shopping centers, and mosque entrances.<sup>[91][92]</sup> In May 2019, Human Rights Watch reported finding Face++ code in the Integrated Joint Operations Platform (IJOP), a police surveillance app used to collect data on, and track the Uighur community in Xinjiang.<sup>[93]</sup> Human Rights Watch released a correction to its report in June 2019 stating that the Chinese company Megvii did not appear to have collaborated on IJOP, and that the Face++ code in the app was inoperable.<sup>[94]</sup> In February 2020, following the Coronavirus outbreak, Megvii applied for a bank loan to optimize the body temperature screening system it had launched to help identify people with symptoms of a Coronavirus infection in crowds. In the loan application Megvii stated that it needed to improve the accuracy of identifying masked individuals.<sup>[95]</sup>

Many public places in China are implemented with facial recognition equipment, including railway stations, airports, tourist attractions, expos, and office buildings. In October 2019, a professor at Zhejiang Sci-Tech University sued the Hangzhou Safari Park for abusing private biometric information of customers. The safari park uses facial recognition technology to verify the identities of its Year Card holders. An estimated 300 tourist sites in China have installed facial recognition systems and use them to admit visitors. This case is reported to be the first on the use of facial recognition systems in China.<sup>[96]</sup> In August 2020 Radio Free Asia reported that in 2019 Geng Guanjun, a citizen of Taiyuan City who had used the WeChat app by Tencent to forward a video to a friend in the United States was subsequently convicted on the charge of the crime "picking quarrels and provoking troubles". The Court documents showed that the Chinese police used a facial recognition system to identify Geng Guanjun as an "overseas democracy activist" and that China's network management and propaganda departments directly monitor WeChat users.<sup>[97]</sup>

In 2019, Protestors in Hong Kong destroyed smart lampposts amid concerns they could contain cameras and facial recognition system used for surveillance by Chinese authorities.<sup>[98]</sup>

## India

Even though facial recognition technology (FRT) is not fully accurate,<sup>[99]</sup> it is being increasingly deployed for identification purposes by the police in India. FRT systems generate a probability match score, or a confidence score between the suspect who is to be identified and the database of identified criminals that is available with the police. The National Automated Facial Recognition System (AFRS)<sup>[100]</sup> is already being developed by the National Crime Records Bureau (NCRB), a body constituted under the Ministry of Home Affairs. The project seeks to develop and deploy a national database of photographs which would comport with a facial recognition technology system by the central and state security agencies. The Internet Freedom Foundation has flagged concerns regarding the project.<sup>[101]</sup> The NGO has highlighted that the accuracy of FRT systems are "routinely exaggerated and the real numbers leave much to be desired."<sup>[101]</sup> The implementation of such faulty FRT systems would lead to high rates of false positives and false negatives in this recognition process."

Under the Supreme Court of India's decision in [[Justice K.S. Puttaswamy vs Union of India (2017 10 SCC 1), any justifiable intrusion by the State into people's right to privacy, which is protected as a fundamental right under Article 21 of the Constitution, must confirm to certain thresholds, namely: legality, necessity, proportionality and procedural safeguards.<sup>[102]</sup> As per the Internet Freedom Foundation, the National Automated Facial Recognition System (AFRS) proposal fails to meet any of these thresholds, citing "absence of legality," "manifest arbitrariness," and "absence of safeguards and accountability."<sup>[103]</sup>

While the national level AFRS project is still in the works, police departments in various states in India are already deploying facial recognition technology systems, such as: TSCOP + CCTNS in Telangana,<sup>[104]</sup> Punjab Artificial Intelligence System (PAIS) in Punjab,<sup>[105]</sup> Trinetra in Uttar Pradesh,<sup>[106]</sup> Police Artificial Intelligence System in Uttarakhand,<sup>[107]</sup> AFRS in Delhi, Automated Multimodal Biometric Identification System (AMBIS) in Maharashtra, FaceTagr in Tamil Nadu. The Crime and Criminal Tracking Network and Systems (CCTNS), which is a Mission Mode Project under the National e-Governance Plan (NeGP),<sup>[108]</sup> is viewed as a system which would connect police stations across India, and help them "talk"<sup>[109]</sup> to each other. The project's objective is to digitize all FIR-related information, including FIRs registered, as well as cases investigated, charge sheets filed, and suspects and wanted persons in all police stations. This shall constitute a national database of crime and criminals in India. CCTNS is being implemented without a data protection law in place. CCTNS is proposed to be integrated with the AFRS, a repository of all crime and criminal related facial data which can be deployed to purportedly identify or verify a person from a variety of inputs ranging from images to videos.<sup>[110]</sup> This has raised privacy concerns from civil society organizations and privacy experts. Both the projects have been censured as instruments of "mass surveillance" at the hands of the state.<sup>[111]</sup> In Rajasthan, 'RajCop,' a police app has been recently integrated with a facial recognition module which can match the face of a suspect against a database of known persons in real-time. Rajasthan police is in currently working to widen the ambit of this module by making it mandatory to upload photographs of all arrested persons in CCTNS database, which will "help develop a rich database of known offenders."<sup>[112]</sup>

Helmets fixed with camera have been designed and being used by Rajasthan police in law and order situations to capture police action and activities of "the miscreants, which can later serve as evidence during the investigation of such cases."<sup>[112]</sup> PAIS (Punjab Artificial Intelligence System), App employs deep learning, machine learning, and face recognition for the identification of criminals to assist police personnel.<sup>[112]</sup> The state of Telangana has installed 8 lakh CCTV cameras,<sup>[112]</sup> with its capital city Hyderabad slowly turning into a surveillance capital.<sup>[113]</sup>

A false positive happens when facial recognition technology misidentifies a person to be someone they are not, that is, it yields an incorrect positive result. They often results in discrimination and strengthening of existing biases. For example, in 2018, Delhi Police reported that its FRT system had an accuracy rate of 2%, which sank to 1% in 2019. The FRT system even failed to distinguish accurately between different sexes.<sup>[114]</sup>

The government of Delhi in collaboration with Indian Space Research Organisation (ISRO) is developing a new technology called Crime Mapping Analytics and Predictive System (CMAPS). The project aims to deploy space technology for "controlling crime and maintaining law and order."<sup>[112]</sup> The system will be connected to a database containing data of criminals.<sup>[112]</sup> The technology is envisaged to be deployed to collect real-time data at the crime scene.<sup>[112]</sup>

In a reply dated November 25, 2020 to a Right to Information request filed by the Internet Freedom Foundation seeking information about the facial recognition system being used by the Delhi Police (with reference number DEPOL/R/E/20/07128),<sup>[115]</sup> the Office of the Deputy Commissioner of Police cum Public Information Officer: Crime stated that they cannot provide the information under section 8(d) of the Right to Information Act, 2005.<sup>[116]</sup> A Right to Information (RTI) request dated July 30, 2020 was filed with the Office of the Commissioner, Kolkata Police, seeking information about the facial recognition technology that the department was using.<sup>[117]</sup> The information sought was denied<sup>[118]</sup> stating that the department was exempted from disclosure under section 24(4) of the RTI Act.

## Latin America

In the 2000 Mexican presidential election, the Mexican government employed face recognition software to prevent voter fraud. Some individuals had been registering to vote under several different names, in an attempt to place multiple votes. By comparing new face images to those already in the voter database, authorities were able to reduce duplicate registrations.<sup>[119]</sup>

In Colombia public transport busses are fitted with a facial recognition system by FaceFirst Inc to identify passengers that are sought by the National Police of Colombia. FaceFirst Inc also built the facial recognition system for Tocumen International Airport in Panama. The face recognition system is deployed to identify individuals among the travelers that are sought by the Panamanian National Police or Interpol.<sup>[120]</sup> Tocumen International Airport operates an airport-wide surveillance system using hundreds of live face recognition cameras to identify wanted individuals passing through the airport. The face recognition system was initially installed as part of a US\$11 million contract and included a computer cluster of sixty computers, a fiber-optic cable network for the airport buildings, as well as the installation of 150 surveillance cameras in the airport terminal and at about 30 airport gates.<sup>[121]</sup>

At the 2014 FIFA World Cup in Brazil the Federal Police of Brazil used face recognition goggles. Face recognition systems "made in China" were also deployed at the 2016 Summer Olympics in Rio de Janeiro.<sup>[120]</sup> Nuctech Company provided 145 inspection terminals for Maracanã Stadium and 55 terminals for the Deodoro Olympic Park.<sup>[122]</sup>

## European Union

Police forces in at least 21 countries of the European Union use, or plan to use, facial recognition systems, either for administrative or criminal purposes.<sup>[123]</sup>

## Greece

Greek police passed a contract with Intracom-Telecom for the provision of at least 1,000 devices equipped with live facial recognition system. The delivery is expected before the summer 2021. The total value of the contract is over 4 million euros, paid for in large part by the Internal Security Fund of the European Commission.<sup>[124]</sup>

## Italy

Italian police acquired a face recognition system in 2017, Sistema Automatico Riconoscimento Immagini (SARI). In November 2020, the Interior ministry announced plans to use it in real-time to identify people suspected of seeking asylum.<sup>[125]</sup>

## The Netherlands

The Netherlands has deployed facial recognition and artificial intelligence technology since 2016.<sup>[126]</sup> The database of the Dutch police currently contains over 2.2 million pictures of 1.3 million Dutch citizens. This accounts for about 8% of the population. In The Netherlands, face recognition is not used by the police on municipal CCTV.<sup>[127]</sup>

## South Africa

In South Africa, in 2016, the city of Johannesburg announced it was rolling out smart CCTV cameras complete with automatic number plate recognition and facial recognition.<sup>[128]</sup>

## Deployment in retail stores

The US firm 3VR, now Identiv, is an example of a vendor which began offering facial recognition systems and services to retailers as early as 2007.<sup>[129]</sup> In 2012 the company advertised benefits such as "dwell and queue line analytics to decrease customer wait times", "facial surveillance analytic[s] to facilitate personalized customer greetings by employees" and the ability to "[c]reate loyalty programs by combining Point of sale (POS) data with facial recognition".<sup>[130]</sup>

## United States

In 2018 the National Retail Federation Loss Prevention Research Council called facial recognition technology "a promising new tool" worth evaluating.<sup>[131]</sup>

In July 2020, the Reuters news agency reported that during the 2010s the pharmacy chain Rite Aid had deployed facial recognition video surveillance systems and components from FaceFirst, DeepCam LLC, and other vendors at some retail locations in the United States.<sup>[131]</sup> Cathy Langley, Rite Aid's vice president of asset protection, used the phrase "feature matching" to refer to the systems and said that usage of the systems resulted in less violence and organized crime in the company's stores, while former vice president of asset protection Bob Oberosler emphasized improved safety for staff and a reduced need for the involvement of law enforcement organizations.<sup>[131]</sup> In a 2020 statement to Reuters in response to the reporting, Rite Aid said that it had ceased using the facial recognition software and switched off the cameras.<sup>[131]</sup>

According to director Read Hayes of the National Retail Federation Loss Prevention Research Council, Rite Aid's surveillance program was either the largest or one of the largest programs in retail.<sup>[131]</sup> The Home Depot, Menards, Walmart, and 7-Eleven are among other US retailers also engaged in large-scale pilot programs or deployments of facial recognition technology.<sup>[131]</sup>

Of the Rite Aid stores examined by Reuters in 2020, those in communities where people of color made up the largest racial or ethnic group were three times as likely to have the technology installed,<sup>[131]</sup> raising concerns related to the substantial history of racial segregation and racial profiling in the United States. Rite Aid said that the selection of locations was "data-driven", based on the theft histories of individual stores, local and national crime data, and site infrastructure.<sup>[131]</sup>

## Additional uses

At the American football championship game Super Bowl XXXV in January 2001, police in Tampa Bay, Florida used Viisage face recognition software to search for potential criminals and terrorists in attendance at the event. 19 people with minor criminal records were potentially identified.<sup>[132][133]</sup>

Face recognition systems have also been used by photo management software to identify the subjects of photographs, enabling features such as searching images by person, as well as suggesting photos to be shared with a specific contact if their presence were detected in a photo.<sup>[134][135]</sup> By 2008 facial recognition systems were typically used as access control in security systems.<sup>[136]</sup>

The United States' popular music and country music celebrity Taylor Swift surreptitiously employed facial recognition technology at a concert in 2018. The camera was embedded in a kiosk near a ticket booth and scanned concert-goers as they entered the facility for known stalkers.<sup>[137]</sup>

On August 18, 2019, *The Times* reported that the UAE-owned Manchester City hired a Texas-based firm, Blink Identity, to deploy facial recognition systems in a driver program. The club has planned a single super-fast lane for the supporters at the Etihad stadium.<sup>[138]</sup> However, civil rights groups cautioned the club against the introduction of this technology, saying that it would risk "normalising a mass surveillance tool". The policy and campaigns officer at Liberty, Hannah Couchman said that Man City's move is alarming, since the fans will be obliged to share deeply sensitive personal information with a private company, where they could be tracked and monitored in their everyday lives.<sup>[139]</sup>

In August 2020, amid the COVID-19 pandemic in the United States, American football stadiums of New York and Los Angeles announced the installation of facial recognition for upcoming matches. The purpose is to make the entry process as touchless as possible.<sup>[140]</sup> Disney's Magic Kingdom, near Orlando, Florida, likewise announced a test of facial recognition technology to create a touchless experience during the pandemic; the test was originally slated to take place between March 23 and April 23, 2021, but the limited timeframe had been removed as of late April.<sup>[141]</sup>



Disney's Magic Kingdom, near Orlando, Florida, during a trial of a facial recognition technology for park entry.

## Advantages and disadvantages

### Compared to other biometric systems

In 2006, the performance of the latest face recognition algorithms was evaluated in the Face Recognition Grand Challenge (FRGC). High-resolution face images, 3-D face scans, and iris images were used in the tests. The results indicated that the new algorithms are 10 times more accurate than the face recognition algorithms of 2002 and 100 times more accurate than those of 1995. Some of the algorithms were able to outperform human participants in recognizing faces and could uniquely identify identical twins.<sup>[35][142]</sup>



One key advantage of a facial recognition system that it is able to perform mass identification as it does not require the cooperation of the test subject to work. Properly designed systems installed in airports, multiplexes, and other public places can identify individuals among the crowd, without passers-by even being aware of the system.<sup>[143]</sup> However, as compared to other biometric techniques, face recognition may not be most reliable and efficient. Quality measures are very important in facial recognition systems as large degrees of variations are possible in face images. Factors such as illumination, expression, pose and noise during face capture can affect the performance of facial recognition systems.<sup>[143]</sup> Among all biometric systems, facial recognition has the highest false acceptance and rejection rates,<sup>[143]</sup> thus questions have been raised on the effectiveness of face recognition software in cases of railway and airport security.<sup>[144]</sup>

## Weaknesses

Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute in 2008, describes one obstacle related to the viewing angle of the face: "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as you go towards profile, there've been problems."<sup>[35]</sup> Besides the pose variations, low-resolution face images are also very hard to recognize. This is one of the main obstacles of face recognition in surveillance systems.<sup>[145]</sup>

Face recognition is less effective if facial expressions vary. A big smile can render the system less effective. For instance: Canada, in 2009, allowed only neutral facial expressions in passport photos.<sup>[146]</sup>

There is also inconstancy in the datasets used by researchers. Researchers may use anywhere from several subjects to scores of subjects and a few hundred images to thousands of images. It is important for researchers to make available the datasets they used to each other, or have at least a standard dataset.<sup>[147]</sup>

Facial recognition systems have been criticized for upholding and judging based on a binary gender assumption.<sup>[148][149][150][151][152][153][154][155][156]</sup> When classifying the faces of cisgender individuals into male or female, these systems are often very accurate,<sup>[148]</sup> however were typically confused or unable to determine the gender identity of transgender and non-binary people.<sup>[148]</sup> Gender norms are being upheld by these systems, so much so that even when shown a photo of a cisgender male with long hair, algorithms was split between following the gender norm of males having short hair, and the masculine facial features and became confused.<sup>[148][156]</sup> This accidental misgendering of people can be very harmful for those who do not identify with their sex assigned at birth, by disregarding and invalidating their gender identity. This is also harmful for people who do not ascribe to traditional and outdated gender norms, because it invalidates their gender expression, regardless of their gender identity.

## Ineffectiveness

Critics of the technology complain that the London Borough of Newham scheme has, as of 2004, never recognized a single criminal, despite several criminals in the system's database living in the Borough and the system has been running for several years. "Not once, as far as the police know, has Newham's automatic face recognition system spotted a live target."<sup>[133][157]</sup> This information seems to conflict with claims that the system was credited with a 34% reduction in crime (hence why it was rolled out to Birmingham also).<sup>[158]</sup>

An experiment in 2002 by the local police department in Tampa, Florida, had similarly disappointing results.<sup>[133]</sup> A system at Boston's Logan Airport was shut down in 2003 after failing to make any matches during a two-year test period.<sup>[159]</sup>

In 2014, Facebook stated that in a standardized two-option facial recognition test, its online system scored 97.25% accuracy, compared to the human benchmark of 97.5%.<sup>[160]</sup>

Systems are often advertised as having accuracy near 100%; this is misleading as the studies often use much smaller sample sizes than would be necessary for large scale applications. Because facial recognition is not completely accurate, it creates a list of potential matches. A human operator must then look through these potential matches and studies show the operators pick the correct match out of the list only about half the time. This causes the issue of targeting the wrong suspect.<sup>[78][161]</sup>

## Controversies

---

### Privacy violations

Civil rights organizations and privacy campaigners such as the Electronic Frontier Foundation, Big Brother Watch and the ACLU express concern that privacy is being compromised by the use of surveillance technologies.<sup>[162][72][163]</sup> Face recognition can be used not just to identify an individual, but also to unearth other personal data associated with an individual – such as other photos featuring the individual, blog posts, social media profiles, Internet behavior, and travel patterns.<sup>[164]</sup> Concerns have been raised over who would have access to the knowledge of one's whereabouts and people with them at any given time.<sup>[165]</sup> Moreover, individuals have limited ability to avoid or thwart face recognition tracking unless they hide their faces. This fundamentally changes the dynamic of day-to-day privacy by enabling any marketer, government agency, or random stranger to secretly collect the identities and associated personal information of any individual captured by the face recognition system.<sup>[164]</sup> Consumers may not understand or be aware of what their data is being used for, which denies them the ability to consent to how their personal information gets shared.<sup>[165]</sup>

In July 2015, the United States Government Accountability Office conducted a Report to the Ranking Member, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U.S. Senate. The report discussed facial recognition technology's commercial uses, privacy issues, and the applicable federal law. It states that previously, issues concerning facial recognition technology were discussed and represent the need for updating the privacy laws of the United States so that federal law continually matches the impact of advanced technologies. The report noted that some industry, government, and private organizations were in the process of developing, or have developed, "voluntary privacy guidelines". These guidelines varied between the stakeholders, but their overall aim was to gain consent and inform citizens of the intended use of facial recognition technology. According to the report the voluntary privacy guidelines helped to counteract the privacy concerns that arise when citizens are unaware of how their personal data gets put to use.<sup>[165]</sup>

In 2016 Russian company NtechLab caused a privacy scandal in the international media when it launched the FindFace face recognition system with the promise that Russian users could take photos of strangers in the street and link them to a social media profile on the social media platform Vkontakte (VT).<sup>[166]</sup> In December 2017, Facebook rolled out a new feature that notifies a user when someone uploads a photo that includes what Facebook thinks is their face, even if they are not tagged. Facebook has attempted to frame the new functionality in a positive light, amidst prior backlashes.<sup>[167]</sup> Facebook's head of privacy, Rob Sherman, addressed this new feature as one that gives people more control over their photos online. "We've thought about this as a really empowering feature," he says. "There may be photos that exist that you don't know about."<sup>[168]</sup> Facebook's DeepFace has become the subject of several class action lawsuits under the Biometric Information Privacy Act, with claims alleging that Facebook is collecting and storing face recognition data of its users without obtaining informed consent, in direct violation of the 2008 Biometric Information Privacy Act (BIPA).<sup>[169]</sup> The most recent case was dismissed in January 2016 because the court lacked jurisdiction.<sup>[170]</sup> In the US, surveillance companies such as Clearview AI are relying on the First Amendment to the United States Constitution to data scrape user accounts on social media platforms for data that can be used in the development of facial recognition systems.<sup>[171]</sup>

In 2019 the Financial Times first reported that facial recognition software was in use in the King's Cross area of London.<sup>[172]</sup> The development around London's King's Cross mainline station includes shops, offices, Google's UK HQ and part of St Martin's College. According to the UK Information Commissioner's Office: "Scanning people's faces as they lawfully go about their daily lives, in order to identify them, is a potential threat to privacy that should concern us all."<sup>[173][174]</sup> The UK Information Commissioner Elizabeth Denham launched an investigation into the use of the King's Cross facial recognition system, operated by the company Argent. In September 2019 it was announced by Argent that facial recognition software would no longer be used at King's Cross. Argent claimed that the software had been deployed between May 2016 and March 2018 on two cameras covering a pedestrian street running through the centre of the development.<sup>[175]</sup> In October 2019 a report by the deputy London mayor Sophie Linden revealed that in a secret deal the Metropolitan Police had passed photos of seven people to Argent for use in their King's cross facial recognition system.<sup>[176]</sup>

Automated Facial Recognition was trialled by the South Wales Police on multiple occasions between 2017 and 2019. The use of the technology was challenged in court by a private individual, Edward Bridges, with support from the charity Liberty (case known as R (Bridges) v Chief Constable South Wales Police). The case was heard in the Court of Appeal and a judgement was given in August 2020.<sup>[177]</sup> The case argued that the use of Facial Recognition was a privacy violation on the basis that there was insufficient legal framework or proportionality in the use of Facial Recognition and that its use was in violation of the Data Protection Acts 1998 and 2018. The case was decided in favour of Bridges and did not award damages. The case was settled via a declaration of wrongdoing.<sup>[177]</sup> In response to the case, the British Government has repeatedly attempted to pass a Bill regulating the use of Facial Recognition in public spaces. The proposed Bills have attempted to appoint a Commissioner with the ability to regulate Facial Recognition use by Government Services in a similar manner to the Commissioner for CCTV. Such a Bill has yet to come into force [correct as of September 2021].<sup>[105]</sup>

## Imperfect technology in law enforcement

It is still contested as to whether or not facial recognition technology works less accurately on people of color.<sup>[178]</sup> One study by Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research) found that the error rate for gender recognition for women of color within three commercial facial recognition systems ranged from 23.8% to 36%, whereas for lighter-skinned men it was between 0.0 and 1.6%. Overall accuracy rates for identifying men (91.9%) were higher than for women (79.4%), and none of the systems accommodated a non-binary understanding of gender.<sup>[179]</sup> It also showed that the datasets used to train commercial facial recognition models were unrepresentative of the broader population and skewed toward lighter-skinned males. However, another study showed that several commercial facial recognition software sold to law enforcement offices around the country had a lower false non-match rate for black people than for white people.<sup>[180]</sup>

Experts fear that face recognition systems may actually be hurting citizens the police claims they are trying to protect.<sup>[181]</sup> It is considered an imperfect biometric, and in a study conducted by Georgetown University researcher Clare Garvie, she concluded that "there's no consensus in the scientific community that it provides a positive identification of somebody."<sup>[182]</sup> It is believed that with such large margins of error in this technology, both legal advocates and facial recognition software companies say that the technology should only supply a portion of the case – no evidence that can lead to an arrest of an individual.<sup>[182]</sup> The lack of regulations holding facial recognition technology companies to requirements of racially biased testing can be a significant flaw in the adoption of use in law enforcement. CyberExtruder, a company that markets itself to law enforcement said that they had not performed testing or research on bias in their software. CyberExtruder did note that some skin colors are more difficult for the software to recognize with current limitations of the technology. "Just as individuals with very dark skin are hard to identify with high significance via facial recognition, individuals with very pale skin are the same," said Blake Senftner, a senior software engineer at CyberExtruder.<sup>[182]</sup>

The United State's National Institute of Standards and Technology (NIST) carried out extensive testing of FRT system 1:1 verification<sup>[183]</sup> and 1:many identification.<sup>[183]</sup> It also tested for the differing accuracy of FRT across different demographic groups. The independent study concluded at present, no FRT system has 100% accuracy.<sup>[184]</sup>

## Data protection

In 2010 Peru passed the Law for Personal Data Protection, which defines biometric information that can be used to identify an individual as sensitive data. In 2012 Colombia passed a comprehensive Data Protection Law which defines biometric data as sensitive information.<sup>[120]</sup> According to Article 9(1) of the EU's 2016 General Data Protection Regulation (GDPR) the processing of biometric data for the purpose of "uniquely identifying a natural person" is sensitive and the facial recognition data processed in this way becomes sensitive personal data. In response to the GDPR passing into the law of EU member states, EU based researchers voiced concern that if they were required under the GDPR to obtain individual's consent for the processing of their facial recognition data, a face database on the scale of MegaFace could never be established again.<sup>[185]</sup> In September 2019 the Swedish Data Protection Authority (DPA) issued its first ever financial penalty for a violation of the EU's General Data Protection Regulation (GDPR) against a school that was using the technology to replace time-consuming roll calls during class. The DPA found that the school illegally obtained the biometric data of its students without completing an impact assessment. In addition the school did not make the DPA aware of the pilot scheme. A 200,000 SEK fine (€19,000/\$21,000) was issued.<sup>[186]</sup>

In the United States of America several U.S. states have passed laws to protect the privacy of biometric data. Examples include the Illinois Biometric Information Privacy Act (BIPA) and the California Consumer Privacy Act (CCPA).<sup>[187]</sup> In March 2020 California residents filed a class action against Clearview AI, alleging that the company had illegally collected biometric data online and with the help of face recognition technology built up a database of biometric data which was sold to companies and police forces. At the time Clearview AI already faced two lawsuits under BIPA<sup>[188]</sup> and an investigation by the Privacy Commissioner of Canada for compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA).<sup>[189]</sup>

## Bans on the use of facial recognition technology

In May 2019, San Francisco, California became the first major United States city to ban the use of facial recognition software for police and other local government agencies' usage.<sup>[190]</sup> San Francisco Supervisor, Aaron Peskin, introduced regulations that will require agencies to gain approval from the San Francisco Board of Supervisors to purchase surveillance technology.<sup>[191]</sup> The regulations also require that agencies publicly disclose the intended use for new surveillance technology.<sup>[191]</sup> In June 2019, Somerville, Massachusetts became the first city on the East Coast to ban face surveillance software for government use,<sup>[192]</sup> specifically in police investigations and municipal surveillance.<sup>[193]</sup> In July 2019, Oakland, California banned the usage of facial recognition technology by city departments.<sup>[194]</sup>

The American Civil Liberties Union ("ACLU") has campaigned across the United States for transparency in surveillance technology<sup>[193]</sup> and has supported both San Francisco and Somerville's ban on facial recognition software. The ACLU works to challenge the secrecy and surveillance with this technology.<sup>[195]</sup>

In January 2020, the European Union suggested, but then quickly scrapped, a proposed moratorium on facial recognition in public spaces.<sup>[196][197]</sup>

During the George Floyd protests, use of facial recognition by city government was banned in Boston, Massachusetts.<sup>[198]</sup> As of June 10, 2020, municipal use has been banned in:<sup>[4]</sup>

- [Berkeley, California](#)
- [Oakland, California](#)
- [Boston, Massachusetts](#) – June 30, 2020<sup>[199]</sup>
- [Brookline, Massachusetts](#)
- [Cambridge, Massachusetts](#)
- [Northampton, Massachusetts](#)
- [Springfield, Massachusetts](#)
- [Somerville, Massachusetts](#)
- [Portland, Oregon](#) – September 2020<sup>[200]</sup>

The West Lafayette, Indiana City Council passed an ordinance banning facial recognition surveillance technology.<sup>[201]</sup>

On October 27, 2020, 22 human rights groups called upon the [University of Miami](#) to ban facial recognition technology. This came after the students accused the school of using the software to identify student protesters. The allegations were, however, denied by the university.<sup>[202]</sup>

The European "[Reclaim Your Face](#)" coalition launched in October 2020. The coalition calls for a ban on facial recognition and launched a [European Citizens' Initiative](#) in February 2021. More than 60 organizations call on the [European Commission](#) to strictly regulate the use of [biometric surveillance technologies](#).<sup>[203]</sup>

A state police reform law in Massachusetts will take effect in July 2021; a ban passed by the legislature was rejected by governor [Charlie Baker](#).<sup>[204]</sup> Instead, the law requires a judicial warrant, limit the personnel who can perform the search, record data about how the technology is used, and create a commission to make recommendations about future regulations.<sup>[205]</sup>

## Emotion recognition

---

In the 18th and 19th century the belief that facial expressions revealed the moral worth or true inner state of a human was widespread and [physiognomy](#) was a respected science in the Western world. From the early 19th century onwards photography was used in the physiognomic analysis of facial features and facial expression to detect [insanity and dementia](#).<sup>[206]</sup> In the 1960s and 1970s the study of human emotions and its expressions was reinvented by [psychologists](#), who tried to define a normal range of emotional responses to events.<sup>[207]</sup> The research on automated [emotion recognition](#) has since the 1970s focused on [facial expressions](#) and [speech](#), which are regarded as the two most important ways in which humans communicate [emotions](#) to other humans. In the 1970s the [Facial Action Coding System](#) (FACS) categorization for the physical expression of emotions was established.<sup>[208]</sup> Its developer [Paul Ekman](#) maintains that there are six emotions that are universal to all human beings and that these can be coded in facial expressions.<sup>[209]</sup> Research into automatic emotion specific expression recognition has in the past decades focused on frontal view images of human faces.<sup>[210]</sup>

In 2016 facial feature emotion recognition algorithms were among the new technologies, alongside [high-definition CCTV](#), [high resolution 3D face recognition](#) and [iris recognition](#), that found their way out of university research labs.<sup>[211]</sup> In 2016 Facebook acquired [FacioMetrics](#), a facial feature emotion recognition corporate spin-off by [Carnegie Mellon University](#). In the same year [Apple Inc.](#) acquired the facial feature emotion recognition start-up [Emotient](#).<sup>[212]</sup> By the end of 2016 commercial vendors of facial recognition systems offered to integrate and deploy emotion recognition algorithms for facial features.<sup>[213]</sup> The [MIT's Media Lab](#) spin-off [Affectiva](#)<sup>[214]</sup> by late 2019 offered a facial expression emotion detection product that can recognize emotions in humans while [driving](#).<sup>[212]</sup>



# Anti-facial recognition systems

---

In January 2013 Japanese researchers from the [National Institute of Informatics](#) created 'privacy visor' glasses that use nearly infrared light to make the face underneath it unrecognizable to face recognition software.<sup>[215]</sup> The latest version uses a titanium frame, light-reflective material and a mask which uses angles and patterns to disrupt facial recognition technology through both absorbing and bouncing back light sources.<sup>[216][217][218][219]</sup> Some projects use [adversarial machine learning](#) to come up with new printed patterns that confuse existing face recognition software.<sup>[220]</sup>

Another method to protect from facial recognition systems are specific haircuts and make-up patterns that prevent the used algorithms to detect a face, known as [computer vision dazzle](#).<sup>[221]</sup> Incidentally, the makeup styles popular with [Juggalos](#) can also protect against facial recognition.<sup>[222]</sup>

Facial masks that are worn to protect from contagious viruses can reduce the accuracy of facial recognition systems. A 2020 [NIST](#) study tested popular one-to-one matching systems and found a failure rate between five and fifty percent on masked individuals. *The Verge* speculated that the accuracy rate of mass surveillance systems, which were not included in the study, would be even less accurate than the accuracy of one-to-one matching systems.<sup>[223]</sup> The facial recognition of [Apple Pay](#) can work through many barriers, including heavy makeup, thick beards and even sunglasses, but fails with masks.<sup>[224]</sup>

## See also

---

- [AI effect](#)
- [Amazon Rekognition](#)
- [Applications of artificial intelligence](#)
- [Automatic number plate recognition](#)
- [Biometric technology in access control](#)
- [Coke Zero Facial Profiler](#)
- [Computer processing of body language](#)
- [Computer vision](#)
- [DeepFace](#)
- [Face perception](#)
- [Face Recognition Grand Challenge](#)
- [FindFace](#)
- [Glasgow Face Matching Test](#)
- [ISO/IEC 19794-5](#)
- [MALINTENT](#)
- [National biometric id card](#)
- [Artificial intelligence for video surveillance](#)
- [Multimedia information retrieval](#)
- [Multilinear subspace learning](#)
- [Pattern recognition, analogy and case-based reasoning](#)
- [Retinal scan](#)
- [SenseTime](#)
- [Super recognisers](#)
- [Template matching](#)
- [Three-dimensional face recognition](#)
- [Vein matching](#)
- [Gait analysis](#)

## Lists

- [List of computer vision topics](#)
- [List of emerging technologies](#)
- [Outline of artificial intelligence](#)

## References

---

1. Chen, S.K; Chang, Y.H (2014). *2014 International Conference on Artificial Intelligence and Software Engineering (AISE2014)*. DEStech Publications, Inc. p. 21. [ISBN 9781605951508](#).
2. Bramer, Max (2006). *Artificial Intelligence in Theory and Practice: IFIP 19th World Computer Congress, TC 12: IFIP AI 2006 Stream, August 21–24, 2006, Santiago, Chile*. Berlin: Springer Science+Business Media. p. 395. [ISBN 9780387346540](#).
3. "Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees" (<https://www.gao.gov/products/gao-21-105309>). [www.gao.gov](https://www.gao.gov). Retrieved September 5, 2021.
4. "IBM bows out of facial recognition market -" (<https://gcn.com/articles/2020/06/10/ibm-quits-facial-recognition.aspx>). GCN. June 10, 2020. Retrieved October 7, 2021.
5. Rachel Metz. "Facebook is shutting down its facial recognition software" (<https://www.cnn.com/2021/11/02/tech/facebook-shuts-down-facial-recognition/index.html>). CNN. Retrieved November 5, 2021.
6. Hill, Kashmir; Mac, Ryan (November 2, 2021). "Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System" (<https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html>). *The New York Times*. [ISSN 0362-4331](#) (<https://www.worldcat.org/issn/0362-4331>). Retrieved November 5, 2021.
7. Nilsson, Nils J. (2009). *The Quest for Artificial Intelligence*. Cambridge University Press. [ISBN 9781139642828](#).
8. de Leeuw, Karl; Bergstra, Jan (2007). *The History of Information Security: A Comprehensive Handbook*. Elsevier. p. 266. [ISBN 9780444516084](#).
9. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. pp. 48–49. [ISBN 9780814732090](#).
10. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. pp. 49–50. [ISBN 9780814732090](#).
11. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. p. 52. [ISBN 9780814732090](#).
12. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. p. 53. [ISBN 9780814732090](#).
13. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. p. 54. [ISBN 9780814732090](#).
14. Malay K. Kundu; Sushmita Mitra; Debasis Mazumdar; Sankar K. Pal, eds. (2012). *Perception and Machine Intelligence: First Indo-Japan Conference, PerMI 2012, Kolkata, India, January 12–13, 2011, Proceedings*. Springer Science & Business Media. p. 29. [ISBN 9783642273865](#).
15. Wechsler, Harry (2009). Malay K. Kundu; Sushmita Mitra (eds.). *Reliable Face Recognition Methods: System Design, Implementation and Evaluation*. Springer Science & Business Media. pp. 11–12. [ISBN 9780387384641](#).
16. Jun Wang; Laiwan Chan; DeLiang Wang, eds. (2012). *Neural Information Processing: 13th International Conference, ICONIP 2006, Hong Kong, China, October 3-6, 2006, Proceedings, Part II*. Springer Science & Business Media. p. 198. [ISBN 9783540464822](#).
17. Wechsler, Harry (2009). *Reliable Face Recognition Methods: System Design, Implementation and Evaluation*. Springer Science & Business Media. p. 12. [ISBN 9780387384641](#).

18. Wechsler, Harry (2009). Malay K. Kundu; Sushmita Mitra (eds.). *Reliable Face Recognition Methods: System Design, Implementation and Evaluation*. Springer Science & Business Media. p. 12. ISBN 9780387384641.
19. Malay K. Kundu; Sushmita Mitra; Debasis Mazumdar; Sankar K. Pal, eds. (2012). *Perception and Machine Intelligence: First Indo-Japan Conference, PerMIn 2012, Kolkata, India, January 12–13, 2011, Proceedings*. Springer Science & Business Media. p. 29. ISBN 9783642273865.
20. "Mugspot Can Find A Face In The Crowd – Face-Recognition Software Prepares To Go To Work In The Streets" (<https://www.sciencedaily.com/releases/1997/11/971112070100.htm>). *ScienceDaily*. November 12, 1997. Retrieved November 6, 2007.
21. Malay K. Kundu; Sushmita Mitra; Debasis Mazumdar; Sankar K. Pal, eds. (2012). *Perception and Machine Intelligence: First Indo-Japan Conference, PerMIn 2012, Kolkata, India, January 12–13, 2011, Proceedings*. Springer Science & Business Media. p. 29. ISBN 9783642273865.
22. Li, Stan Z.; Jain, Anil K. (2005). *Handbook of Face Recognition*. Springer Science & Business Media. pp. 14–15. ISBN 9780387405957.
23. Kumar Datta, Asit; Datta, Madhura; Kumar Banerjee, Pradipta (2015). *Face Detection and Recognition: Theory and Practice*. CRC. p. 123. ISBN 9781482226577.
24. Li, Stan Z.; Jain, Anil K. (2005). *Handbook of Face Recognition*. Springer Science & Business Media. p. 1. ISBN 9780387405957.
25. Li, Stan Z.; Jain, Anil K. (2005). *Handbook of Face Recognition*. Springer Science & Business Media. p. 2. ISBN 9780387405957.
26. "Airport Facial Recognition Passenger Flow Management" (<http://www.hrsid.com/company/technology/face-recognition>). *hrsid.com*.
27. Bonsor, K. (September 4, 2001). "How Facial Recognition Systems Work" (<http://computer.howstuffworks.com/facial-recognition.htm>). Retrieved June 2, 2008.
28. Smith, Kelly. "Face Recognition" (<https://www.biometrics.gov/Documents/FaceRec.pdf>) (PDF). Retrieved June 4, 2008.
29. R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates", *IEEE Trans. on PAMI*, 1993, (15)10:1042–1052
30. R. Brunelli, *Template Matching Techniques in Computer Vision: Theory and Practice*, Wiley, ISBN 978-0-470-51706-2, 2009 ([1] (<http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470517069.html>) TM book)
31. Zhang, David; Jain, Anil (2006). *Advances in Biometrics: International Conference, ICB 2006, Hong Kong, China, January 5–7, 2006, Proceedings*. Berlin: Springer Science & Business Media. p. 183. ISBN 9783540311119.
32. "A Study on the Design and Implementation of Facial Recognition Application System". *International Journal of Bio-Science and Bio-Technology*.
33. H. Ugail, *Deep face recognition using full and partial face images*, Elsevier, ISBN 978-0-12-822109-9, 2022 (<https://doi.org/10.1016/B978-0-12-822109-9.00015-1>] *Advanced Methods and Deep Learning in Computer Vision*)
34. Harry Wechsler (2009). *Reliable Face Recognition Methods: System Design, Implementation and Evaluation*. Springer Science & Business Media. p. 196. ISBN 9780387384641.
35. Williams, Mark. "Better Face-Recognition Software" (<http://www.technologyreview.com/Infotech/h18796/?a=f>). Retrieved June 2, 2008.
36. Crawford, Mark. "Facial recognition progress report" (<http://spie.org/x57306.xml>). SPIE Newsroom. Retrieved October 6, 2011.
37. Kimmel, Ron. "Three-dimensional face recognition" (<https://www.cs.technion.ac.il/~ron/PAPERS/BroBroKimIJCV05.pdf>) (PDF). Retrieved January 1, 2005.

38. Duhn, S. von; Ko, M. J.; Yin, L.; Hung, T.; Wei, X. (September 1, 2007). "Three-View Surveillance Video Based Face Modeling for Recognition [sic]". *Three-View Surveillance Video Based Face Modeling for Recognition*. pp. 1–6. doi:10.1109/BCC.2007.4430529 (<https://doi.org/10.1109%2FBCC.2007.4430529>). ISBN 978-1-4244-1548-9. S2CID 25633949 (<https://api.semanticscholar.org/CorpusID:25633949>).
39. Socolinsky, Diego A.; Selinger, Andrea (January 1, 2004). "Thermal Face Recognition in an Operational Scenario" (<http://dl.acm.org/citation.cfm?id=1896300.1896448>). CVPR'04. IEEE Computer Society. pp. 1012–1019 – via ACM Digital Library.
40. "Army Builds Face Recognition Technology that Works in Low-Light Conditions" (<https://www.azorobotics.com/News.aspx?newsID=9840>). *AZoRobotics*. April 18, 2018. Retrieved August 17, 2018.
41. Thirimachos Bourlai (2016). *Face Recognition Across the Imaging Spectrum*. Springer. p. 142. ISBN 9783319285016.
42. Thirimachos Bourlai (2016). *Face Recognition Across the Imaging Spectrum*. Springer. p. 140. ISBN 9783319285016.
43. "Army develops face recognition technology that works in the dark" (<https://www.arl.army.mil/www/default.cfm?article=3199>). *Army Research Laboratory*. April 16, 2018. Retrieved August 17, 2018.
44. Riggan, Benjamin; Short, Nathaniel; Hu, Shuowen (March 2018). "Thermal to Visible Synthesis of Face Images using Multiple Regions" (<https://www.researchgate.net/publication/323932058>). *ResearchGate*. arXiv:1803.07599 (<https://arxiv.org/abs/1803.07599>). Bibcode: 2018arXiv180307599R (<https://ui.adsabs.harvard.edu/abs/2018arXiv180307599R>).
45. Cole, Sally (June 2018). "U.S. Army's AI facial recognition works in the dark". *Military Embedded Systems*. p. 8.
46. Shontell, Alyson (September 15, 2015). "Snapchat buys Lookery, a 2-year-old startup that lets you Photoshop your face while you video chat" (<http://www.businessinsider.sg/snapchat-buys-lookery-2015-9/>). *Business Insider Singapore*. Retrieved April 9, 2018.
47. Kumar Mandal, Jyotsna; Bhattacharya, Debika (2019). *Emerging Technology in Modelling and Graphics: Proceedings of IEM Graph 2018*. Springer. p. 672. ISBN 9789811374036.
48. Simonite, Tom. "Facebook Creates Software That Matches Faces Almost as Well as You Do" (<https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/>). *MIT Technology Review*. Retrieved April 9, 2018.
49. "Facebook's DeepFace shows serious facial recognition skills" (<https://www.cbsnews.com/news/facebooks-deepface-shows-serious-facial-recognition-skills/>). Retrieved April 9, 2018.
50. "Why Facebook is beating the FBI at facial recognition" (<https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition>). *The Verge*. Retrieved April 9, 2018.
51. "How TikTok's 'For You' Algorithm Actually Works" (<https://www.wired.com/story/tiktok-finally-explains-for-you-algorithm-works>). *Wired*. ISSN 1059-1028 (<https://www.worldcat.org/issn/1059-1028>). Retrieved April 17, 2021.
52. "How TikTok recommends videos #ForYou" (<https://web.archive.org/web/20200618171925/http://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you>). TikTok. June 18, 2020. Archived from the original (<https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you>) on June 18, 2020. Retrieved April 22, 2021.
53. "TikTok agrees legal payout over facial recognition" (<https://web.archive.org/web/20210226160803/https://www.bbc.com/news/technology-56210052>). *BBC News*. February 26, 2021. Archived from the original (<https://www.bbc.com/news/technology-56210052>) on February 26, 2021. Retrieved April 22, 2021.
54. "A glimpse at bank branches of the future: video walls, booth-sized locations and 24/7 access" (<https://www.usatoday.com/story/money/2018/07/24/bank-branch-future/796748002/>). *USA Today*. Retrieved August 13, 2018.

55. Heater, Brian. "Don't rely on Face Unlock to keep your phone secure" (<https://techcrunch.com/2017/09/06/dont-rely-on-face-unlock-to-keep-your-phone-secure/>). *TechCrunch*. Retrieved November 2, 2017.
56. "Galaxy S8 face recognition already defeated with a simple picture" (<https://arstechnica.com/gadgets/2017/03/video-shows-galaxy-s8-face-recognition-can-be-defeated-with-a-picture/>). *Ars Technica*. Retrieved November 2, 2017.
57. "How Facial Recognition Works in Xbox Kinect" (<https://www.wired.com/2010/11/how-facial-recognition-works-in-xbox-kinect/>). *Wired*. Retrieved November 2, 2017.
58. "Windows 10 says 'Hello' to logging in with your face and the end of passwords" (<https://arstechnica.com/information-technology/2015/03/windows-10-says-hello-to-logging-in-with-your-face-and-the-end-of-passwords/>). *Ars Technica*. March 17, 2015. Retrieved March 17, 2015.
59. Kubota, Yoko (September 27, 2017). "Apple iPhone X Production Woe Sparked by Juliet and Her Romeo" (<https://www.wsj.com/articles/apple-iphone-x-production-woe-sparked-by-juliet-and-her-romeo-1506510189?mod=e2twd>). *The Wall Street Journal*. Archived (<https://web.archive.org/web/20170928103032/https://www.wsj.com/articles/apple-iphone-x-production-woe-sparked-by-juliet-and-her-romeo-1506510189?mod=e2twd>) from the original on September 28, 2017. Retrieved September 27, 2017.
60. Kubota, Yoko (September 27, 2017). "Apple iPhone X Production Woe Sparked by Juliet and Her Romeo" (<https://www.wsj.com/articles/apple-iphone-x-production-woe-sparked-by-juliet-and-her-romeo-1506510189>). *The Wall Street Journal*. ISSN 0099-9660 (<https://www.worldcat.org/issn/0099-9660>). Retrieved April 10, 2018.
61. "The five biggest questions about Apple's new facial recognition system" (<https://www.theverge.com/2017/9/12/16298156/apple-iphone-x-face-id-security-privacy-police-unlock>). *The Verge*. Retrieved April 10, 2018.
62. "Apple's Face ID Feature Works With Most Sunglasses, Can Be Quickly Disabled to Thwart Thieves" (<https://www.macrumors.com/2017/09/14/face-id-works-with-sunglasses-thwarts-thieves/>). Retrieved April 10, 2018.
63. Heisler, Yoni (November 3, 2017). "Infrared video shows off the iPhone X's new Face ID feature in action" (<http://bgr.com/2017/11/03/iphone-x-face-id-video-infrared/>). *BGR*. Retrieved April 10, 2018.
64. "Modi govt now plans a 'touchless' vaccination process, with Aadhaar-based facial recognition" (<https://theprint.in/health/modi-govt-now-plans-a-touchless-vaccination-process-with-aadhaar-based-facial-recognition/634719/>). *ThePrint*. Retrieved February 12, 2022.
65. "Despite Privacy Fears, Aadhaar-Linked Facial Recognition Used For Covid-19 Vaccines" (<https://inc42.com/buzz/despite-privacy-fears-facial-recognition-used-for-covid-19-vaccines/>). *Inc42*. Retrieved February 12, 2022.
66. "Joint Statement: Say no to Aadhaar based Facial Recognition for Vaccination!" (<https://internetfreedom.in/sign-on-and-support-close-to-10-organisations-and-158-individuals-who-are-warning-against-aadhaar-based-facial-recognition-for-vaccination/>). *Internet Freedom Foundation*. Retrieved February 12, 2022.
67. "Panoptic Tracker, Finance (Pension Cell) Department, Government of Meghalaya" (<https://panoptic.in/meghalaya/FRT-000068>). *Panoptic Project*. Retrieved February 12, 2022.
68. "Meghalaya clarifies on controversial app: 'Facial Recognition Technology doesn't require any anchoring legislation'" (<https://indianexpress.com/article/north-east-india/meghalaya/meghalaya-pensioner-app-facial-recognition-7629818/>). *Indian Express*. Retrieved February 12, 2022.
69. "Smartgates Face editing for the mins of the can we have" (<https://www.abf.gov.au/entering-and-leaving-australia/smartgates/arrivals>). *Australian Border Force*. Retrieved March 11, 2019.
70. "Our history" (<https://www.customs.govt.nz/about-us/about-customs/our-history/>). *New Zealand Customs Service*. Retrieved March 11, 2019.
71. "Facial recognition technology is coming to Canadian airports this spring" (<http://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344>). *CBC News*. Retrieved March 3, 2017.



72. "Face Off: The lawless growth of facial recognition in UK policing" (<https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>) (PDF). *Big Brother Watch*.
73. Anthony, Sebastian (June 6, 2017). "UK police arrest man via automatic face-recognition tech" (<https://arstechnica.com/tech-policy/2017/06/police-automatic-face-recognition/>). *Ars Technica*.
74. Rees, Jenny (September 4, 2019). "Police use of facial recognition ruled lawful" (<https://www.bbc.com/news/uk-wales-49565287>). Retrieved November 8, 2019.
75. Burgess, Matt (January 24, 2020). "The Met Police will start using live facial recognition across London" (<https://www.wired.co.uk/article/london-met-police-facial-recognition>). *Wired UK*. ISSN 1357-0978 (<https://www.worldcat.org/issn/1357-0978>). Retrieved January 24, 2020.
76. Danica Kirka (August 11, 2020). "UK court says face recognition violates human rights" (<http://techxplore.com/news/2020-08-uk-court-recognition-violates-human.html>). *TechPlore*. Retrieved October 4, 2020.
77. Fortune. "Here's How Many Adult Faces Are Scanned From Facial Recognition Databases" (<http://fortune.com/2016/10/18/facial-recognition-database/>).
78. "The trouble with facial recognition technology (in the real world)" (<http://phys.org/news/2016-12-facial-recognition-technology-real-world.html>).
79. "Real-Time Facial Recognition Is Available, But Will U.S. Police Buy It?" (<https://www.npr.org/2018/05/10/609422158/real-time-facial-recognition-is-available-but-will-u-s-police-buy-it>). NPR.
80. "Police Facial Recognition Databases Log About Half Of Americans" (<https://www.npr.org/2016/10/23/499042369/police-facial-recognition-databases-log-about-half-of-americans>). NPR.
81. Knezevich, Kevin Rector, Alison. "Maryland's use of facial recognition software questioned by researchers, civil liberties advocates" (<http://www.baltimoresun.com/news/maryland/crime/bs-md-facial-recognition-20161017-story.html>).
82. "Next Generation Identification" ([https://www.fbi.gov/about-us/cjis/fingerprints\\_biometrics/ngi](https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi)). FBI. Retrieved April 5, 2016.
83. ICE Uses Facial Recognition To Sift State Driver's License Records, Researchers Say (<https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa>).
84. "TSA had expressed its intention to adopt a similar program for domestic air travel" (<https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/>). *USA Today*. August 16, 2019.
85. Shen, Xinmei (October 4, 2018). "'Skynet', China's massive video surveillance network" (<http://www.scmp.com/abacus/who-what/what/article/3028246/skynet-chinas-massive-video-surveillance-network>). *South China Morning Post*. Retrieved December 13, 2020.
86. Chan, Tara Francis (March 27, 2018). "16 parts of China are now using Skynet" (<https://www.businessinsider.com.au/china-facial-recognition-technology-works-in-one-second-2018-3>). *Business Insider*. Retrieved December 13, 2020.
87. "From ale to jail: facial recognition catches criminals at China beer festival" (<https://www.theguardian.com/world/2017/sep/01/facial-recognition-china-beer-festival>). *The Guardian*. September 1, 2017. Retrieved March 8, 2018.
88. "Police use facial recognition technology to detect wanted criminals during beer festival in Chinese city of Qingdao" (<https://web.archive.org/web/20171116082821/http://opengovasia.com/articles/7975-police-use-facial-recognition-technology-to-capture-wanted-criminals-during-beer-festival-in-chinese-city-of-qingdao>). *opengovasia.com*. OpenGovAsia. Archived from the original (<https://www.opengovasia.com/articles/7975-police-use-facial-recognition-technology-to-capture-wanted-criminals-during-beer-festival-in-chinese-city-of-qingdao>) on November 16, 2017. Retrieved March 8, 2018.
89. "Chinese police are using smart glasses to identify potential suspects" (<https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/>). *TechCrunch*. February 8, 2018. Retrieved December 3, 2020.

90. "Beijing police are using facial-recognition glasses to identify car passengers and number plates" (<https://www.businessinsider.com/china-police-using-smart-glasses-facial-recognition-2018-3>). *Business Insider*. March 12, 2018. Retrieved December 3, 2020.
91. "China's massive investment in artificial intelligence has an insidious downside" (<http://www.sciencemag.org/news/2018/02/china-s-massive-investment-artificial-intelligence-has-insidious-downside>). *Science AAAS*. February 7, 2018. Retrieved February 23, 2018.
92. "China bets on facial recognition in big drive for total surveillance" (<https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/>). *The Washington Post*. 2018. Retrieved February 23, 2018.
93. Liao, Rita (May 8, 2019). "Alibaba-backed facial recognition startup Megvii raises \$750 million" (<https://techcrunch.com/2019/05/08/megvii-750-million/>). *TechCrunch*. Retrieved August 28, 2019.
94. Dai, Sarah (June 5, 2019). "AI unicorn Megvii not behind app used for surveillance in Xinjiang, says human rights group" (<https://www.scmp.com/tech/start-ups/article/3013229/ai-unicorn-megvii-not-behind-app-used-surveillance-xinjiang-says>). *South China Morning Post*. Retrieved August 28, 2019.
95. Cheng Leng, Yingzhi Yang and Ryan Woo (February 20, 2020). "Exclusive: Hundreds of Chinese businesses seek billions in loans to contend with coronavirus" ([https://mobile.reuters.com/article/amp/idUSKBN204182?\\_\\_twitter\\_impression=true](https://mobile.reuters.com/article/amp/idUSKBN204182?__twitter_impression=true)). *Reuters*. Retrieved October 5, 2020.
96. "A lawsuit against face-scans in China could have big consequences" (<https://www.economist.com/china/2019/11/09/a-lawsuit-against-face-scans-in-china-could-have-big-consequences>). *The Economist*. November 9, 2019.
97. Xiaoshan, Huang; Wen, Cheng. "New evidence showing Tencent monitors overseas users" (<https://web.archive.org/web/20200816050851/https://www.rfa.org/cantonese/news/wechat-08142020065757.html>). Archived from the original (<https://www.rfa.org/cantonese/news/wechat-08142020065757.html>) on August 16, 2020. Retrieved August 15, 2020.
98. Zak Doffman (August 26, 2019). "Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine" (<https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/>). *Forbes*. Retrieved December 3, 2020.
99. Lohr, Steve (February 9, 2018). "Facial Recognition Is Accurate, if You're a White Guy" (<https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html>). *The New York Times*. ISSN 0362-4331 (<https://www.worldcat.org/issn/0362-4331>). Retrieved February 14, 2022.
100. "NCRB's National Automated Facial Recognition System" (<https://panoptic.in/>). *panoptic.in*. Retrieved February 14, 2022.
101. "Watch the Watchmen Series Part 4 : The National Automated Facial Recognition System" (<https://internetfreedom.in/watch-the-watchmen-series-part-4-the-national-automated-facial-recognition-system/>). *Internet Freedom Foundation*. October 7, 2020. Retrieved February 14, 2022.
102. "Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018" (<https://indiankanoon.org/doc/127517806/>). *Indian Kanoon*.
103. "We might be in the market for a new kind of face mask" (<https://internetfreedom.in/maskon/>). *Internet Freedom Foundation*. July 18, 2019. Retrieved February 14, 2022.
104. Barik, Soumyarendra (October 22, 2019). "'Fingerprint is not a big issue': Hyderabad police on collecting biometrics of 'suspects'" (<https://www.medianama.com/2019/10/223-hyd-police-on-collecting-biometrics-of-suspects/>). *MediaNama*. Retrieved February 14, 2022.
105. "Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] - Parliamentary Bills - UK Parliament" (<https://bills.parliament.uk/bills/2610>). *bills.parliament.uk*. Retrieved September 10, 2021.

106. "UP Police launch 'Trinetra', its AI-powered face recognition app to catch criminals" (<https://www.financialexpress.com/industry/technology/up-police-launch-trinetra-its-ai-powered-face-recognition-app-to-catch-criminals/1426618/>). *The Financial Express*. Retrieved February 14, 2022.
107. "Uttarakhand Police acquire face recognition software to help nab criminals" (<https://www.hindustantimes.com/dehradun/uttarakhand-police-acquire-face-recognition-software-to-help-nab-criminals/story-hIO0dmwRfOcK9npC0IMjtM.html>). *Hindustan Times*. August 27, 2018. Retrieved February 14, 2022.
108. "Crime and Criminal Tracking Network & Systems (CCTNS) | National Crime Records Bureau" (<https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns>). *ncrb.gov.in*. Retrieved February 18, 2022.
109. "CCTNS Project to let police stations 'talk': where it stands, and how it can help fight crime" (<https://indianexpress.com/article/explained/cctns-project-to-let-police-stations-talk-where-it-stands-and-how-it-can-help-fight-crime/>). *The Indian Express*. November 20, 2015. Retrieved February 18, 2022.
110. "Home Ministry moves to get automated facial recognition system for police" (<https://www.hindustantimes.com/india-news/home-ministry-moves-to-get-automated-facial-recognition-system-for-police/story-AfPOydDwKwz0leTt3t4WvI.html>). *Hindustan Times*. July 8, 2019. Retrieved February 18, 2022.
111. "IFF's Legal Notice to the NCRB on the Revised RFP for the National Automated Facial Recognition System" (<https://internetfreedom.in/iffs-legal-notice-to-the-ncrb-on-the-revised-rfp-for-the-national-automated-facial-recognition-system/>). *Internet Freedom Foundation*. July 15, 2020. Retrieved February 18, 2022.
112. *PARLIAMENT OF INDIA. RAJYA SABHA. TWO HUNDRED THIRTY SEVENTH REPORT ON POLICE - TRAINING, MODERNISATION AND REFORMS* ([https://rajyasabha.nic.in/rsnew/Committee\\_site/Committee\\_File/ReportFile/15/161/237\\_2022\\_2\\_17.pdf](https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/15/161/237_2022_2_17.pdf)) (PDF). DEPARTMENT-RELATED PARLIAMENTARY STANDING COMMITTEE ON HOME AFFAIRS, India. 2022. p. 34.
113. U. Sudhakar Reddy (November 10, 2021). "8.3 lakh cameras in Telangana, Hyderabad turning into surveillance city: Amnesty | Hyderabad News - Times of India" (<https://timesofindia.indiatimes.com/city/hyderabad/8-3l-cameras-in-t-hyd-turning-into-surveillance-city-amnesty/articleshow/87615657.cms>). *The Times of India*. Retrieved February 18, 2022.
114. "Indian govt's approach to facial recognition is flawed & driven by faulty assumptions" (<https://theprint.in/opinion/indian-govt-approach-to-facial-recognition-flawed-driven-by-faulty-assumptions/327036/>). *ThePrint*. November 27, 2019. Retrieved February 15, 2022.
115. "Right to Information Updates from Delhi Police, Kolkata Police and Telangana State Technology Services" (<https://panoptic.in/>). *panoptic.in*. Retrieved February 15, 2022.
116. "Section 8(1)(d) in The Right To Information Act, 2005" (<https://indiankanoon.org/doc/1838023/>). *Indian Kanoon*.
117. "Project Panoptic: RTI Updates from Delhi Police, Kolkata Police and Telangana State Technology Services" (<https://internetfreedom.in/project-panoptic-right-to-information-updates/>). *Internet Freedom Foundation*. December 1, 2020. Retrieved February 15, 2022.
118. Chunduru, Aditya (December 2, 2020). "RTI: Kolkata, Delhi police refuse to give information on facial recognition systems" (<https://www.medianama.com/2020/12/223-rti-replies-delhi-kolkata-police-telangana-facial-recognition-iff/>). *MediaNama*. Retrieved February 15, 2022.
119. "Mexican Government Adopts FaceIt Face Recognition Technology to Eliminate Duplicate Voter Registrations in Upcoming Presidential Election" (<https://web.archive.org/web/20160305151832/http://www.thefreelibrary.com/Mexican+Government+Adopts+FaceIt+Face+Recognition+Technology+to...-a062019954>). Business Wire. May 11, 2000. Archived from the original (<http://www.thefreelibrary.com/Mexican+Government+Adopts+FaceIt+Face+Recognition+Technology+to...-a062019954>) on March 5, 2016. Retrieved June 2, 2008.
120. Selinger, Evan; Polonetsky, Jules; Tene, Omer (2018). *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press. p. 112. ISBN 9781316859278.

121. Vogel, Ben. "Panama puts names to more faces" (<http://www.ihsairport360.com/article/4812/panama-puts-names-to-more-faces>). IHS Jane's Airport Review. Archived (<https://web.archive.org/web/20141012185226/http://www.ihsairport360.com/article/4812/panama-puts-names-to-more-faces>) from the original on October 12, 2014. Retrieved October 7, 2014.
122. "'Made-in-China' products shine at Rio Olympics" ([http://english.www.gov.cn/news/photos/2016/08/15/content\\_281475417902847.htm](http://english.www.gov.cn/news/photos/2016/08/15/content_281475417902847.htm)). The State Council, The people's Republic of China. August 15, 2016. Retrieved November 14, 2020.
123. Kayser-Bril, Nicolas (December 11, 2019). "At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals" (<https://algorithmwatch.org/en/story/face-recognition-police-europe/>). *AlgorithmWatch*.
124. Pedriti, Corina (January 28, 2021). "Flush with EU funds, Greek police to introduce live face recognition before the summer" (<https://algorithmwatch.org/en/story/greek-police-live-facial-recognition/>). *AlgorithmWatch*.
125. Coluccini, Riccardo (January 13, 2021). "Lo scontro Viminale-Garante della privacy sul riconoscimento facciale in tempo reale" (<https://irpimedia.irpi.eu/viminale-garante-privacy-riconoscimento-facciale-in-tempo-reale/>). *IrpiMedia*.
126. Techredacteur, Joost Schellevis. "Politie gaat verdachten opsporen met gezichtsherkenning" (<https://nos.nl/nl/2148598>). *nos.nl* (in Dutch). Retrieved September 22, 2019.
127. Boon, Lex (August 25, 2018). "Meekijken met de 226 gemeentecamera's" (<https://www.parool.nl/gs-b111d648>). *Het Parool* (in Dutch). Retrieved September 22, 2019.
128. How CCTV surveillance poses a threat to privacy in South Africa (<https://theconversation.com/how-cctv-surveillance-poses-a-threat-to-privacy-in-south-africa-97418>)
129. Ross, Tim (2007). "3VR Featured on Fox Business News" (<https://www.youtube.com/watch?v=iV-MPQ0Zra0>). *Money for Breakfast* (Interview). Fox Business. "Interviewer: Now, can I buy something like this? Is this... do you really restrict the customers for this? Tim Ross: It's primarily being purchased by banks, retailers, and the government today and is sold through a variety of security channels."
130. "Improve Customer Service" (<https://web.archive.org/web/20120814071615/http://www.3vr.com/solutions/grow/improve-customer-service>). 3VR. Archived from the original (<http://www.3vr.com/solutions/grow/improve-customer-service>) on August 14, 2012. "3VR's Video Intelligence Platform (VIP) transforms customer service by allowing businesses to: • Optimize staffing decisions, increase sales conversion rates and decrease customer wait times by bringing extraordinary clarity to the analysis of traffic patterns • Align staffing decisions with actual customer activity, using dwell and queue line analytics to decrease customer wait times • Increase competitiveness by using 3VR's facial surveillance analytic to facilitate personalized customer greetings by employees • Create loyalty programs by combining point of sale (POS) data with facial recognition"
131. Dastin, Jeffrey L.; Cadell, Cate; Yang, Yizhing; Tham, Engen; Goh, Brenda; Master, Farah; Jackson, Lucas; Michalska, Aleksandra; Hart, Samuel (July 28, 2020). Marquis, Julie; Robinson, Simon (eds.). "Special Report: Rite Aid deployed facial recognition systems in hundreds of U.S. stores" (<https://www.reuters.com/article/us-usa-riteaid-software-specialreport/special-report-rite-aid-deployed-facial-recognition-systems-in-hundreds-of-u-s-stores-idUSKCN24T1HL>). U.S. Legal News. *Reuters*. Further reporting by Paresh Dave, Tom Bergin, and the Reuters Beijing and Shanghai newsrooms; data analysis by Ryan McNeill. Archived (<https://web.archive.org/web/20201219022523/https://www.reuters.com/article/us-usa-riteaid-software-specialreport/special-report-rite-aid-deployed-facial-recognition-systems-in-hundreds-of-u-s-store-s-idUSKCN24T1HL>) from the original on December 19, 2020.

132. Greene, Lisa (February 15, 2001). "Face scans match few suspects" ([http://www.sptimes.com/News/021601/TampaBay/Face\\_scans\\_match\\_few\\_.shtml](http://www.sptimes.com/News/021601/TampaBay/Face_scans_match_few_.shtml)) (SHTML). *St. Petersburg Times*. Archived ([https://web.archive.org/web/20141130123749/http://www.sptimes.com/News/021601/TampaBay/Face\\_scans\\_match\\_few\\_.shtml](https://web.archive.org/web/20141130123749/http://www.sptimes.com/News/021601/TampaBay/Face_scans_match_few_.shtml)) from the original on November 30, 2014. Retrieved June 30, 2011. "By using Viisage software, police matched 19 people's faces to photos of people arrested in the past for minor pickpocketing, fraud and other charges. They weren't charged with any game-day misdeeds. THIS IS A FARCE"
133. Krause, Mike (January 14, 2002). "Is face recognition just high-tech snake oil?" (<http://www.enterstageright.com/archive/articles/0102/0102facerecog.htm>). *Enter Stage Right*. ISSN 1488-1756 (<https://www.worldcat.org/issn/1488-1756>). Archived (<https://web.archive.org/web/20020124050149/http://www.enterstageright.com/archive/articles/0102/0102facerecog.htm>) from the original on January 24, 2002. Retrieved June 30, 2011.
134. "Windows 10's Photos app is getting smarter image search just like Google Photos" (<https://www.theverge.com/2017/7/28/16055418/microsoft-windows-10-photos-app-ai-image-sorting>). *The Verge*. Retrieved November 2, 2017.
135. Perez, Sarah. "Google Photos upgraded with new sharing features, photo books, and Google Lens" (<https://techcrunch.com/2017/05/17/google-photos-upgraded-with-new-sharing-features-photo-books-and-google-lens/>). *TechCrunch*. Retrieved November 2, 2017.
136. "Face Recognition Applications" (<https://web.archive.org/web/20080713020541/http://www.animetrics.com/Technology/FRApplications.html>). Animetrics. Archived from the original (<http://www.animetrics.com/technology/frapplications.html>) on July 13, 2008. Retrieved June 4, 2008.
137. Giaritelli, Anna (December 13, 2018). "Taylor Swift used airport-style facial recognition on concertgoers" (<https://www.washingtonexaminer.com/news/taylor-swift-used-airport-style-facial-recognition-on-concertgoers>). *washingtonexaminer.com*. Retrieved December 13, 2018.
138. "Manchester City tries facial recognition to beat football queues" (<https://www.thetimes.co.uk/article/manchester-city-tries-facial-recognition-to-beat-football-queues-smdrckrj?ni-statuscode=acsaz-307#>). *The Times*. Retrieved August 18, 2019.
139. "Manchester City warned against using facial recognition on fans" (<https://www.theguardian.com/technology/2019/aug/18/manchester-city-face-calls-to-reconsider-facial-recognition-tech>). *The Guardian*. Retrieved August 18, 2019.
140. Olson, Parmy (August 1, 2020). "Facial Recognition's Next Big Play: the Sports Stadium" (<https://www.wsj.com/articles/facial-recognition-next-big-play-the-sports-stadium-11596290400>). *The Wall Street Journal*. ISSN 0099-9660 (<https://www.worldcat.org/issn/0099-9660>). Retrieved August 3, 2020.
141. "Facial Recognition Technology Test" (<https://web.archive.org/web/20210422135841/https://disneyworld.disney.go.com/guest-services/park-entry-test/>). *Walt Disney World Park Entry Technology Test*. Disney. Archived from the original (<https://disneyworld.disney.go.com/guest-services/park-entry-test/>) on April 22, 2021. Retrieved April 22, 2021.
142. R. Kimmel and G. Sapiro (April 30, 2003). "The Mathematics of Face Recognition" (<https://web.archive.org/web/20070715175109/http://www.siam.org/news/news.php?id=309>). SIAM News. Archived from the original (<http://siam.org/news/news.php?id=309>) on July 15, 2007. Retrieved April 30, 2003.
143. "Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice" (<https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/>). *Bayometric*. January 23, 2017. Retrieved April 10, 2018.
144. (PDF) <https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf> (<https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf>). {{cite web}}: Missing or empty |title= (help)
145. Haghghat, Mohammad; Abdel-Mottaleb, Mohamed (2017). "Low Resolution Face Recognition in Surveillance Systems Using Discriminant Correlation Analysis". *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*. pp. 912–917. doi:10.1109/FG.2017.130 (<https://doi.org/10.1109%2FFG.2017.130>). ISBN 978-1-5090-4023-0. S2CID 36639614 (<https://api.semanticscholar.org/CorpusID:36639614>).



146. "Passport Canada – Photos" (<https://web.archive.org/web/20090301054020/http://www.ppt.gc.ca/cdn/photos.aspx?lang=eng>). [passportcanada.gc.ca](http://www.ppt.gc.ca/cdn/photos.aspx?lang=eng). Archived from the original (<http://www.ppt.gc.ca/cdn/photos.aspx?lang=eng>) on March 1, 2009.
147. Albiol, A., Albiol, A., Oliver, J., Mossi, J.M.(2012). Who is who at different cameras: people re-identification using depth cameras (<https://riunet.upv.es/bitstream/handle/10251/56627/kinect.pdf?sequence=3>). *Computer Vision, IET*. Vol 6(5), 378–387.
148. "Facial recognition software has a gender problem" ([https://www.nsf.gov/discoveries/disc\\_summary.jsp?cntn\\_id=299486](https://www.nsf.gov/discoveries/disc_summary.jsp?cntn_id=299486)). *nsf.gov*. Retrieved May 9, 2021.
149. Rehnman, Jenny. "The role of gender in face recognition" (<https://www.diva-portal.org/smash/get/diva2:196786/FULLTEXT01.pdf>) (PDF): 69.
150. Mishra, Maruti V.; Likitlersuang, Jirapat; Wilmer, Jeremy B.; Cohan, Sarah; Germine, Laura; DeGutis, Joseph M. (November 29, 2019). "Gender Differences in Familiar Face Recognition and the Influence of Sociocultural Gender Inequality" (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6884510>). *Scientific Reports*. **9** (1): 17884. Bibcode:2019NatSR...917884M (<https://ui.adsabs.harvard.edu/abs/2019NatSR...917884M>). doi:10.1038/s41598-019-54074-5 (<https://doi.org/10.1038/s41598-019-54074-5>). ISSN 2045-2322 (<https://www.worldcat.org/issn/2045-2322>). PMC 6884510 (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6884510>). PMID 31784547 (<https://pubmed.ncbi.nlm.nih.gov/31784547>).
151. "Facing gender bias in facial recognition technology" (<https://www.helpnetsecurity.com/2020/08/27/facial-recognition-bias/>). *Help Net Security*. August 27, 2020. Retrieved May 9, 2021.
152. Palmer, Matthew A.; Brewer, Neil; Horry, Ruth (March 2013). "Understanding gender bias in face recognition: Effects of divided attention at encoding" (<https://www.sciencedirect.com/science/article/pii/S0001691813000231>). *Acta Psychologica*. **142** (3): 362–369. doi:10.1016/j.actpsy.2013.01.009 (<https://doi.org/10.1016/j.actpsy.2013.01.009>). ISSN 0001-6918 (<https://www.worldcat.org/issn/0001-6918>). PMID 23422290 (<https://pubmed.ncbi.nlm.nih.gov/23422290>).
153. "Why Gender-Neutral Facial Recognition Will Change How We Look at Technology" (<https://www.technologynetworks.com/informatics/articles/why-gender-neutral-facial-recognition-will-change-how-we-look-at-technology-332962>). *Informatics from Technology Networks*. Retrieved May 9, 2021.
154. "Facial Recognition | Gendered Innovations" (<https://genderedinnovations.stanford.edu/case-studies/facial.html>). *genderedinnovations.stanford.edu*. Retrieved May 9, 2021.
155. Mason, Susan E. (September 27, 2007). "Age and gender as factors in facial recognition and identification" (<https://www.tandfonline.com/doi/abs/10.1080/03610738608259453>). *Experimental Aging Research*. **12** (3): 151–154. doi:10.1080/03610738608259453 (<https://doi.org/10.1080/03610738608259453>). PMID 3830234 (<https://pubmed.ncbi.nlm.nih.gov/3830234>).
156. *Facial recognition software has a gender problem* ([https://www.eurekalert.org/pub\\_releases/2019-10/uoca-frs102919.php](https://www.eurekalert.org/pub_releases/2019-10/uoca-frs102919.php)), retrieved May 9, 2021
157. Meek, James (June 13, 2002). "Robo cop" (<https://www.theguardian.com/Archive/Article/0,4273,4432506,00.htm>). London: UK Guardian newspaper.
158. "Birmingham City Centre CCTV Installs Visionics' Facelt" (<https://www.allbusiness.com/government/government-bodies-offices-regional/6111139-1.html>). *Business Wire*. June 2, 2008.

159. Willing, Richard (September 2, 2003). "Airport anti-terror systems flub tests; Face-recognition technology fails to flag 'suspects' " (<https://web.archive.org/web/20071001050407/http://pqasb.pqarchiver.com/USAToday/access/391952771.html?dids=391952771%3A391952771&FMT=ABS&FMTS=ABS%3AFT&date=Sep+2%2C+2003&author=Richard+Willing&pub=USA+TODAY&edition=&startpage=A.03&desc=Airport+anti-terror+systems+flub+tests+%3B+Face-recognition+technology+fails+to+flag+%27suspects%27>). *USA Today*. Archived from the original (<http://pqasb.pqarchiver.com/USAToday/access/391952771.html?dids=391952771:391952771&FMT=ABS&FMTS=ABS:FT&date=Sep+2%2C+2003&author=Richard+Willing&pub=USA+TODAY&edition=&startpage=A.03&desc=Airport+anti-terror+systems+flub+tests+%3B+Face-recognition+technology+fails+to+flag+%27suspects%27>) (Abstract) on October 1, 2007. Retrieved September 17, 2007.
160. Meyer, Robinson (2015). "How Worried Should We Be About Facial Recognition?" (<https://www.theatlantic.com/technology/archive/2015/07/how-good-facial-recognition-technology-government-regulation/397289/>). *The Atlantic*. Retrieved March 2, 2018.
161. White, David; Dunn, James D.; Schmid, Alexandra C.; Kemp, Richard I. (October 14, 2015). "Error Rates in Users of Automatic Face Recognition Software" (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4605725>). *PLOS ONE*. **10** (10): e0139827. Bibcode:2015PLoSO..1039827W (<https://ui.adsabs.harvard.edu/abs/2015PLoSO..1039827W>). doi:10.1371/journal.pone.0139827 (<https://doi.org/10.1371%2Fjournal.pone.0139827>). PMC 4605725 (<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4605725>). PMID 26465631 (<https://pubmed.ncbi.nlm.nih.gov/26465631>).
162. "EFF Sues FBI For Access to Facial-Recognition Records" (<https://www.eff.org/press/releases/eff-sues-fbi-access-facial-recognition-records>). Electronic Frontier Foundation. June 26, 2013.
163. "Q&A On Face-Recognition" (<https://www.aclu.org/technology-and-liberty/qa-face-recognition>). *American Civil Liberties Union*.
164. Harley Geiger (December 6, 2011). "Facial Recognition and Privacy" (<http://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy>). Center for Democracy & Technology. Retrieved January 10, 2012.
165. Cackley, Alicia Puente (July 2015). "FACIAL RECOGNITION TECHNOLOGY Commercial Uses, Privacy Issues, and Applicable Federal Law" (<http://www.gao.gov/assets/680/671764.pdf>) (PDF).
166. Thomas Brewster (September 22, 2020). "This Russian Facial Recognition Startup Plans To Take Its 'Aggression Detection' Tech Global With \$15 Million Backing From Sovereign Wealth Funds" (<https://www.forbes.com/sites/thomasbrewster/2020/09/22/this-russian-facial-recognition-startup-plans-to-take-its-aggression-detection-tech-global-with-15-million-backing-from-sovereign-wealth-funds/>). *Forbes*. Retrieved October 4, 2020.
167. "Singel-Minded: Anatomy of a Backlash, or How Facebook Got an 'F' for Facial Recognition" (<https://www.wired.com/2011/06/anatomy-of-backlash/>). *WIRED*. Retrieved April 10, 2018.
168. "Facebook Can Now Find Your Face, Even When It's Not Tagged" (<https://www.wired.com/story/facebook-will-find-your-face-even-when-its-not-tagged/>). *WIRED*. Retrieved April 10, 2018.
169. "Facebook Keeps Getting Sued Over Face-Recognition Software, And Privacy Groups Say We Should Be Paying More Attention" (<http://www.ibtimes.com/facebook-keeps-getting-sued-over-face-recognition-software-privacy-groups-say-we-2082166>). *International Business Times*. September 3, 2015. Retrieved April 5, 2016.
170. Herra, Dana. "Judge tosses Illinois privacy law class action vs Facebook over photo tagging; California cases still pending" (<http://cookcountyrecord.com/stories/510660138-judge-tosses-illinois-privacy-law-class-action-vs-facebook-over-photo-tagging-california-cases-still-pending>). *cookcountyrecord.com*. Retrieved April 5, 2016.
171. Skinner-Thompson, Scott (2020). *Privacy at the Margins*. Cambridge University Press. p. 110. ISBN 9781107181373.
172. Murgia, Madhumita (August 12, 2019). "London's King's Cross uses facial recognition in security cameras" (<https://www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c>). *Financial Times* (subscription site). Retrieved August 17, 2019.

173. "King's Cross facial recognition investigated" (<https://www.bbc.com/news/technology-49357759>). *BBC News*. August 15, 2019. Retrieved August 17, 2019.
174. Cellan-Jones, Rory (August 16, 2019). "Tech Tent: Is your face on a watch list?" (<https://www.bbc.com/news/technology-49368875>). *BBC News*. Retrieved August 17, 2019.
175. Sabbagh, Dan (September 2, 2019). "Facial recognition technology scrapped at King's Cross site" (<https://www.theguardian.com/technology/2019/sep/02/facial-recognition-technology-scrapped-at-kings-cross-development>). *The Guardian*. ISSN 0261-3077 (<https://www.worldcat.org/issn/0261-3077>). Retrieved September 2, 2019.
176. Sabbagh, Dan (October 4, 2019). "Facial recognition row: police gave King's Cross owner images of seven people" (<https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people>). *The Guardian*. Retrieved October 4, 2020.
177. Judiciary UK (August 11, 2020). "Judgement: Bridges v South Wales Police - Courts and Tribunals Judiciary" (<https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf>) (PDF). *Judiciary UK*. Retrieved September 10, 2021.
178. "Photo Algorithms ID White Men Fine—Black Women, Not So Much" (<https://www.wired.com/story/photo-algorithms-id-white-men-fine-black-women-not-so-much/>). *WIRED*. Retrieved April 10, 2018.
179. Joy Buolamwini; Timnit Gebru (2018). "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (<http://proceedings.mlr.press/v81/buolamwini18a.html>). *Proceedings of Machine Learning Research*. Vol. 81. pp. 77–91. Retrieved March 8, 2018.
180. Grother, Patrick; Quinn, George; Phillips, P. Jonathon (August 24, 2011). "Report on the Evaluation of 2D Still-Image Face Recognition Algorithms" (<https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7709.pdf>) (PDF). *National Institute of Standards and Technology*.
181. Buranyi, Stephen (August 8, 2017). "Rise of the racist robots – how AI is learning all our worst impulses" (<https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>). *The Guardian*. Retrieved April 10, 2018.
182. Brel, Ali (December 4, 2017). "How white engineers built racist code – and why it's dangerous for black people" (<https://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police>). *The Guardian*. Retrieved April 10, 2018.
183. "Face Recognition Vendor Test (FRVT) Ongoing" (<https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing>). *NIST*. December 14, 2016. Retrieved February 15, 2022.
184. Grother, Patrick J.; Ngan, Mei L.; Hanaoka, Kayee K. (December 19, 2019). "Face Recognition Vendor Test Part 3: Demographic Effects" (<https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects>).
185. Ronald Leenes; Rosamunde van Brakel; Serge Gutwirth; Paul de Hert, eds. (2018). *Data Protection and Privacy: The Internet of Bodies*. Bloomsbury Publishing. p. 176. ISBN 9781509926213.
186. "Unlawful Use of Facial Recognition Technology Lead to GDPR Penalty in Sweden" (<https://www.compliancejunction.com/unlawful-use-of-facial-recognition-technology-lead-to-gdpr-penalty-in-sweden/>). *Compliance Junction*. September 1, 2019. Retrieved September 20, 2019.
187. Bock, Lisa (2020). *Identity Management with Biometrics: Explore the latest innovative solutions to provide secure identification and authentication*. Packt Publishing. p. 320. ISBN 9781839213212.
188. Pascu, Luana (March 16, 2020). "California residents file class action against Clearview AI biometric data collection citing CCPA" (<https://www.biometricupdate.com/202003/california-residents-file-class-action-against-clearview-ai-biometric-data-collection-citing-ccpa>). *BiometricUpdate.com*. Retrieved October 25, 2020.
189. Burt, Chris (February 24, 2020). "Canadian Privacy Commissioners investigate Clearview AI, develop guidance for police use of biometrics" (<https://www.biometricupdate.com/202002/canadian-privacy-commissioners-investigate-clearview-ai-develop-guidance-for-police-use-of-biometrics>). *BiometricUpdate.com*. Retrieved October 25, 2020.

190. Conger, Kate; Fausset, Richard; Kovalski, Serge F. (May 14, 2019). "San Francisco Bans Facial Recognition Technology" (<https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>). *The New York Times*. ISSN 0362-4331 (<https://www.worldcat.org/issn/0362-4331>). Retrieved March 26, 2020.
191. "San Francisco Bans Agency Use of Facial Recognition Tech" (<https://www.wired.com/story/san-francisco-bans-use-facial-recognition-tech/>). *Wired*. ISSN 1059-1028 (<https://www.worldcat.org/issn/1059-1028>). Retrieved March 26, 2020.
192. "Somerville Bans Government Use Of Facial Recognition Tech" (<https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech>). *wbur.org*. Retrieved March 26, 2020.
193. "Somerville City Council passes facial recognition ban – The Boston Globe" (<https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html>). *The Boston Globe*. Retrieved March 26, 2020.
194. Haskins, Caroline (July 17, 2019). "Oakland Becomes Third U.S. City to Ban Facial Recognition" ([https://www.vice.com/en\\_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz](https://www.vice.com/en_us/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz)). *Vice*. Retrieved April 11, 2020.
195. Nkonde, Mutale (2019). "Automated Anti-Blackness: Facial Recognition in Brooklyn, New York" (<https://search.proquest.com/docview/2404400349>). *Kennedy School Review*. 20: 30–26. ProQuest 2404400349 (<https://search.proquest.com/docview/2404400349>) – via ProQuest.
196. "EU drops idea of facial recognition ban in public areas: paper" (<https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q>). *Reuters*. January 29, 2020. Retrieved April 12, 2020.
197. "Facial recognition: EU considers ban" (<https://www.bbc.com/news/technology-51148501>). *BBC News*. January 17, 2020. Retrieved April 12, 2020.
198. Boston mayor OKs ban on facial recognition tech (<https://www.bizjournals.com/boston/news/2020/06/30/mayor-walsh-signs-ban-on-facial-recognition-tech.html>)
199. Boston mayor OKs ban on facial recognition tech (<https://www.bizjournals.com/boston/news/2020/06/30/mayor-walsh-signs-ban-on-facial-recognition-tech.html>)
200. Rachel Metz. "Portland passes broadest facial recognition ban in the US" (<https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html>). *CNN*. Retrieved September 13, 2020.
201. "West Lafayette City Council approves ban on facial recognition technology" [2] (<https://www.wfyi.org/news/articles/west-lafayette-city-council-approves-ban-on-facial-recognition-technology>)
202. "Human Rights Groups Call On The University of Miami To Ban Facial Recognition" (<https://www.forbes.com/sites/rachelsandler/2020/10/27/human-rights-groups-call-on-the-university-of-miami-to-ban-facial-recognition/>). *Forbes*. Retrieved October 27, 2020.
203. "Reclaim Your Face: Ban Biometric Mass Surveillance!" (<https://reclaimyourface.eu/>). *Reclaim Your Face*. Retrieved June 12, 2021.
204. Governor signs police overhaul into law (<https://www.bostonglobe.com/2020/12/31/metro/governor-baker-signs-landmark-policing-reform-law/>)
205. Massachusetts is one of the first states to create rules around facial recognition in criminal investigations. (<https://www.nytimes.com/2021/03/01/business/massachusetts-is-one-of-the-first-states-to-create-rules-around-facial-recognition-in-criminal-investigations.html>)
206. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. p. 156. ISBN 9780814732090.
207. Gates, Kelly (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press. p. 161. ISBN 9780814732090.
208. Konar, Amit; Chakraborty, Aruna (2015). *Emotion Recognition: A Pattern Analysis Approach*. John Wiley & Sons. p. 185. ISBN 9781118130667.
209. Konar, Amit; Chakraborty, Aruna (2015). *Emotion Recognition: A Pattern Analysis Approach*. John Wiley & Sons. p. 186. ISBN 9781118130667.

210. Konar, Amit; Chakraborty, Aruna (2015). *Emotion Recognition: A Pattern Analysis Approach*. John Wiley & Sons. p. 187. ISBN 9781118130667.
211. "Facial Recognition Market – Global Forecast to 2021" (<http://www.digitaljournal.com/pr/3187852>). *Digital Journal*. December 30, 2016. Retrieved October 17, 2020.
212. Fowler, Gary (October 14, 2019). "How Emotional AI Is Creating Personalized Customer Experiences And Making A Social Impact" (<https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2019/10/14/how-emotional-ai-is-creating-personalized-customer-experiences-and-making-a-social-impact/>). *Forbes*. Retrieved October 17, 2020.
213. "Facial Recognition Market – Global Forecast to 2021" (<http://www.digitaljournal.com/pr/3187852>). *Digital Journal*. December 30, 2016. Retrieved October 17, 2020.
214. "Eureka Park Returns" ([https://www.nsf.gov/news/news\\_summ.jsp?cntn\\_id=126487&org=NSF&from=news%22](https://www.nsf.gov/news/news_summ.jsp?cntn_id=126487&org=NSF&from=news%22)) (Press release). *National Science Foundation*. January 7, 2013. Retrieved February 3, 2013.
215. "These Goofy-Looking Glasses Could Make You Invisible to Facial Recognition Technology" ([http://www.slate.com/blogs/future\\_tense/2013/01/18/isao\\_echizen\\_and\\_seiichi\\_gohshi\\_s\\_privacy\\_visor\\_shields\\_you\\_from\\_facial.html](http://www.slate.com/blogs/future_tense/2013/01/18/isao_echizen_and_seiichi_gohshi_s_privacy_visor_shields_you_from_facial.html)). *Slate*. January 18, 2013. Retrieved January 22, 2013.
216. Hongo, Jun. "Eyeglasses with Face Un-Recognition Function to Debut in Japan" (<https://blogs.wsj.com/japanrealtime/2015/08/07/eyeglasses-with-face-un-recognition-function-to-debut-in-japan/>). *The Wall Street Journal*. Retrieved February 9, 2017.
217. Osborne, Charlie. "Privacy visor which blocks facial recognition software set for public release" (<https://www.zdnet.com/article/privacy-visor-which-blocks-facial-recognition-software-set-for-public-release/>). *ZDNet*. Retrieved February 9, 2017.
218. Stone, Maddie. "These Glasses Block Facial Recognition Technology" (<https://gizmodo.com/these-glasses-block-facial-recognition-technology-1722826081>). *Gizmodo*. Retrieved February 9, 2017.
219. "How Japan's Privacy Visor fools face-recognition cameras" (<http://www.pcworld.com/article/2969732/privacy/how-japans-privacy-visor-fools-facerecognition-cameras.html>). *PC World*. Retrieved February 9, 2017.
220. Cox, Kate (April 10, 2020). "Some shirts hide you from cameras—but will anyone wear them?" (<https://arstechnica.com/features/2020/04/some-shirts-hide-you-from-cameras-but-will-anyone-wear-them/>). *Ars Technica*. Retrieved April 12, 2020.
221. Harvey, Adam. "CV Dazzle: Camouflage from Face Detection" (<https://cvdazzle.com/>). *cvdazzle.com*. Retrieved September 15, 2017.
222. Schreiber, Hope. "Worried about facial recognition technology? Juggalo makeup prevents involuntary surveillance" (<https://www.yahoo.com/lifestyle/worried-facial-recognition-technology-juggalo-makeup-prevents-involuntary-surveillance-232354372.html>). Retrieved July 18, 2019.
223. Vincent, James (July 28, 2020). "Face masks are breaking facial recognition algorithms, says new government study" (<https://www.theverge.com/2020/7/28/21344751/facial-recognition-face-masks-accuracy-nist-study>). *The Verge*. Retrieved August 27, 2020.
224. Hern, Alex (August 21, 2020). "Face masks give facial recognition software an identity crisis" (<https://www.theguardian.com/technology/2020/aug/21/face-masks-give-facial-recognition-software-identity-crisis>). *The Guardian*. ISSN 0261-3077 (<https://www.worldcat.org/issn/0261-3077>). Retrieved August 24, 2020.

## Further reading


- Farokhi, Sajad; Shamsuddin, Siti Mariyam; Flusser, Jan; Sheikh, U.U; Khansari, Mohammad; Jafari-Khouzani, Kourosh (2014). "Near infrared face recognition by combining Zernike moments and undecimated discrete wavelet transform". *Digital Signal Processing*. **31** (1): 13–27. doi:10.1016/j.dsp.2014.04.008 (<https://doi.org/10.1016%2Fj.dsp.2014.04.008>).
- "The Face Detection Algorithm Set to Revolutionize Image Search" (<http://www.technologyreview.com/view/535201/the-face-detection-algorithm-set-to-revolutionise-image-search/>) (Feb.

2015), *MIT Technology Review*

- Garvie, Clare; Bedoya, Alvaro; Frankle, Jonathan (October 18, 2016). *Perpetual Line Up: Unregulated Police Face Recognition in America* (<https://www.perpetuallineup.org/>). Center on Privacy & Technology at [Georgetown Law](#). Retrieved October 22, 2016.
- "Facial Recognition Software 'Sounds Like Science Fiction,' but May Affect Half of Americans" (<http://www.cbc.ca/radio/asithappens/as-it-happens-friday-edition-1.3814209/facial-recognition-software-sounds-like-science-fiction-but-may-affect-half-of-americans-1.3815754>). *As It Happens*. Canadian Broadcasting Corporation. October 20, 2016. Retrieved October 22, 2016. Interview with Alvaro Bedoya, executive director of the Center on Privacy & Technology at Georgetown Law and co-author of *Perpetual Line Up: Unregulated Police Face Recognition in America*.

## External links

---

-  Media related to [Facial recognition system](#) at Wikimedia Commons
  - A Photometric Stereo Approach to Face Recognition (<https://www.face-six.com/>). The University of the West of England. <http://www1.uwe.ac.uk/et/mvl/projects/facerecognition.aspx>
- 

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Facial\\_recognition\\_system&oldid=1080500094](https://en.wikipedia.org/w/index.php?title=Facial_recognition_system&oldid=1080500094)"

---

**This page was last edited on 1 April 2022, at 17:12.**

Text is available under the Creative Commons Attribution-ShareAlike License 3.0; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.