Working Paper on Facial Recognition Technology

Discussed and adopted
at the 70th Meeting on 29th-30th November 2022 and
71st Meeting on 7th-8th June 2023
Written Procedure after this meeting

Introduction

The Berlin Group recognizes the potential beneficial applications of facial recognition technologies ("FRT"), including in enhancing public safety and security. However, we also acknowledge that technologies have the capability to facilitate intrusive, arbitrary, and illegitimate surveillance. Irresponsible use of FRT has the potential to erode data protection and privacy standards, infringe human rights, and perpetuate discrimination by returning biased results.

We support the resolutions of the Global Privacy Assembly ("GPA") that reaffirmed the privacy, legal, and ethical challenges of FRT and identified the need to address these issues through global standards, technical solutions, and regulatory cooperation. Building on the work of the GPA, this paper describes the attributes of facial recognition technologies; usages in private and public sectors; risks for privacy and data protection; and means to mitigate them. The paper includes recommendations for policy makers and for controllers and processors who use this technology in the public or private sector.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Background

Facial recognition technology is used for recognizing a human face by using biometrics to map facial features from digital files. The technology compares the information extracted from the file with one or more other databases of known faces in order to search for a match. Note that this is distinct from facial analytics – the practice of identifying characteristics such as age, gender, emotion, ethnicity, or other characteristics in a face. Facial analytics may be a component of facial recognition in some cases but are not exclusively used for identification or verification. We have included some discussion of facial analytics in this paper as well but want to make clear that facial analytics have distinct risks since they may not include elements of individual identification or verification.

FRT is widely used for various needs both by private and public sectors (for law enforcement and other public purposes). This includes collaboration on facial recognition between public and private actors.

The use of FRT is becoming more common given the fact that it is possible to integrate it as an add-on to existing systems and the technology has the ability to extract identifying information from a wide variety of image sources, including from online images and from cameras installed in public spaces.

FRT has a huge impact on privacy and the capacity to be highly intrusive due to its ability to process personal biometrics of individuals and, under some circumstances, to indicate the whereabouts of individuals and allow for inferring additional personal information, such as political views, religion, geolocation data, health data, and more.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

These capabilities, or purported capabilities, include significant risks for individuals and groups, such as stalking, improper identification, and risk of criminalization.

Scope

This paper describes the attributes of FRT, usages in private and public sectors, risks for privacy and data protection, and means to mitigate those risks. The paper includes recommendations for policy makers and for controllers and processors who use this technology for public or economic purposes.

While the paper will look in large part at technical elements of FRT, we want to make clear that FRT encompasses not only the technical elements of the systems used (cameras, wired and wireless transmission of data, facial templates and files, algorithms, etc.), but also the interaction and relationships between these and non-technical elements of the system, including policies, regulations, human designers, end users, and subjects.

We have included some discussion of facial analytics in this paper as well, but want to make clear that facial analytics have distinct risks, since they may not include elements of individual identification. These examples are included for the sake of exemplifying how FRT works.

Description of Facial Recognition Technology

Facial recognition can be used to verify or identify individuals by their faces. It is a biometric technology, which identifies individuals by measuring and analyzing facial

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

structure and comparing markers identified in the facial structure to markers of faces held on file or from other sources. FRT converts a photo or video image of a person—often called a probe image—into a template, or a mathematical representation of the face. For some facial recognition functions, if the technology detects a face in the probe image, an algorithm then matches and compares the template to that of another photo and calculates the similarities between the two to estimate the likelihood of a match.[1]

FRT may perform four basic functions:[2]

Detection: recognizing that there is a face in an image.

Verification: confirming the identity associated with a face (e.g. a system that compares the face of a person to the face in a passport) in order to verify that the individual is who they claim to be.[3]

Identification: comparing an image of an unknown face to a gallery of images of known people in order to identify the unknown individual (e.g. a system in a public place captures images of unknown faces and compares the images to images of known people on a watch list).[4]

[1] United States Government Accountability Office, Report to Congressional Requesters, *FACIAL RECOGNITION TECHNOLOGY Privacy and Accuracy Issues Related to Commercial Uses* (July 2020), https://www.gao.gov/assets/710/708201.pdf.
[2] Supra note 1.
[3] This is an example of one-to-one matching, which compares the facial template from a probe image to an existing template or image of the person to verify their identity.
[4] This is an example of one-to-many matching, which compares the facial template from the probe image to a gallery of images of known people of interest.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Facial Analysis: identifying characteristics from a face, such as age, gender, emotions, ethnicity, etc. Note that, since this function is not necessarily used to identify or verify an individual, facial analysis is considered distinct from facial recognition and carries with it distinct risks and pitfalls.

In order to perform identification or verficiation functions, the system captures an image in a digital format (probe), determines that the image contains the image of a face (face detection), creates a facial template (by correcting the image to fit appropriate standards of lighting, color, size, angle, etc. and extracting unique features of the data subject), and performs a facial template matching by comparing the probe template with one or more templates stored in the FRT system.[5] In some cases, the system may also store the information in the system for future comparison, though this is not always the case, for example some systems are limited to real-time comparison only and do not store the incoming data.

FRT is often based on machine learning in which an algorithm is trained on data to build a model that can identify patterns and learn features of faces, such as "what is an important part of the face to understand who the person in the picture is." Theoretically, as the algorithm receives more training data, it becomes more accurate or at least more consistent (assuming it has sufficient capacity). "Accuracy" here typically means fewer false positives and false negatives, with some additional components and considerations.[6]

[5] Supra note 1 above.
[6] Other considerations when determining accuracy include adjusting acceptable thresholds of false positives and false negatives, evaluating false match rates and false non match rates, conducting tests such as the NIST Face Recognition Vendor Test (https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt), etc.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

As a result of the above, high volumes of images are typically deemed necessary to train the algorithm. For this purpose, there are bodies (companies and organizations) that maintain databases of images on which algorithms designed for face recognition systems can be trained.[7]

FRT use requires that personal information be collected and used at multiple stages, including: training an FRT algorithm, creating a face database, collecting probe image(s) to be compared against that database, and possibly others. A legal basis for the use of data and implementing data protection principles as stated in relevant laws must exist for all steps that implicate personal information.

Use

There are a range of common FRT uses in both the public and private sector, but new uses are continually being put into practice. We list some of the most common uses below but note that this is by no means a definitive list and, as you will see, many of the uses have been challenged by activists and Data Protection Authorities ("DPAs").

[7] Consultative Committee Of The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, *Facial Recognition: Current Situation And Challenges*, https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1.

Private Sector

Secure access to premises or devices - FRT can be used as a means of controlling physical access to spaces (using a camera to authenticate a person prior to entering a room, complex, and even a vehicle) or as a data security measure to regulate access to electronic devices, such as unlocking a PC, mobile phone, online account, and more.

The use of FRT for secure access purposes is common in the banking sector (for complying with laws prohibiting money laundering, or to facilitate remote payment, access to applications, and more). In this sector, increased use of face recognition is expected due to changes in the European Union Payment Services Regulation, which includes a requirement for strong means of identification. The regulation requires two stages of identification as a condition for the provision of payment services - one of which can be biometric, including face recognition.

Security monitoring – Many venues use FRT for securing spaces such as casinos, sports stadiums, malls, concert halls, etc. Typically, these systems compare scans of venue entrants against databases of individuals who may be banned or considered dangerous. Stores also use the technology in an attempt to detect thefts. For example, in New Zealand it was discovered that a supermarket chain installed FRT that scans the faces of those entering the store and compares their faces to images that appear in a database, which includes images of individuals who are suspected of

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

having previously stolen in stores.[8] Like New Zealand, in the United States, the RiteAid pharmacy chain installed cameras in stores and used FRT with the intention of deterring theft and protecting staff and customers from violence. The system was deployed in stores that reported high cases of theft.[9]

FRT systems are not always used without opposition and in some cases, data protection authorities have intervened in the use of these systems. In the Netherlands, the DPA sent an official warning to a supermarket that used a system that scanned visitor's faces and compared them to images in a database that included images of people whose entry to the supermarket was prohibited. The Dutch DPA ruled that the use of Live FRT for security purposes is prohibited, apart from exceptional and rare cases.[10] In a similar case in Canada, the British Columbia DPA investigated the use of FRT in four Canadian Tire stores and found it to be unlawful.[11]

Marketing purposes and customer service – Facial recognition is also used by private entities to identify individuals and later send targeted marketing, invitations to customers clubs, customer service, etc. The technology can also be used to identify

[8] The Law Foundation review, Facial Recognition Technology in New Zealand Toward a Legal and Ethical Framework, https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf.
[9] Reuters, *Rite Aid deployed facial recognition systems in hundreds of U.S. stores,* https://www.reuters.com/investigates/special-report/usa-riteaid-software/.
[10] European Data Protection Board, *Dutch DPA issues Formal Warning to a Supermarket for its use of Facial Recognition Technology*, https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en.
[11] Office of the Information and Privacy Commissioner for British Columbia, *Canadian Tire Associate Dealers' use of facial recognition technology,* https://www.oipc.bc.ca/investigation-reports/3785.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

VIP customers and send targeted marketing messages.[12] FRT is also used to purportedly "streamline" customer experiences with different companies. For example, in China, hotels used the technology for check in purposes,[13] and U.S. car rental services have been using FRT in an effort to speed up check in.[14] One fast food chain in the U.S. used FRT to identify customers for quick and repeated orders.[15]

Monitoring attendance – FRT is sometimes used for monitoring the presence of employees or people visiting events. There are also companies that use FRT to monitor attendance at the workplace and on mandatory work events.[16]

Gaming – Some video games allow users to integrate their face into the game to verify their user identity.[17] In addition, many game consoles use control systems based on user movements to provide control over the game. The camera used by the control system may also share the images of users with a face analysis system to estimate the age and gender of the users. This information may change the course of the game to tailor the user's experience according to their profile. The system can

[12] Sean Hargrave, *Facial recognition – a powerful ad tool or privacy nightmare?,* The Guardian (August 17, 2016), https://www.theguardian.com/media-network/2016/aug/17/facial-recognition-a-powerful-ad-tool-or-privacy-nightmare
[13] Esther Hertzfeld, *Facial recognition check-in rolled out at 50 hotels in China,* Hotel Management (September 13, 2018), https://www.hotelmanagement.net/tech/facial-recognition-check-rolled-out-at-50-hotels-china.
[14] Jeff John Roberts, *Hertz and Clear Bring Facial Recognition to the Rental Car Industry,* Fortune (December 11, 2018), https://fortune.com/2018/12/11/hertz-facial-recognition/.
[15] Mark Hamstra, *Tech That Allows Restaurant Customers to 'Pay With Their Face' is Gaining Traction,* Good Company, https://www.uschamber.com/co/good-company/launch-pad/facial-recognition-technology-covid-19.
[16] Linda Rosencrance, *Privacy and security issues associated with facial recognition software,* Tech Republic (August 25, 2022), https://www.techrepublic.com/article/privacy-and-security-issues-associated-with-facial-recognition-software/.
[17] *Privacy Principles for Facial Recognition Technologies*, Future of Privacy Forum (December 2015), https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

prevent access to certain content depending on the estimated age of the user or perform targeted advertising depending on the user's profile.

Facial analysis – Facial analysis systems may theoretically be used for many trait identification purposes and purport to identify characteristics like age, gender, race, mood, and more. Some possible uses that private entities have considered include identifying age to prevent the sale of alcohol to minors, identifying personal characteristics for filtering employees, predicting criminal characteristics in recruitment processes, or identifying emotions, gender, and age for targeted advertising in public places. However, not only is this technology unproven in effectively identifying these traits, but there is also a high risk of misuse, bias, and discrimination in the use of these technologies. As an example of misuse of these systems, "Cia Hering," a local clothing retail company in Brazil, was sued by the Brazil Institute for Consumer Protection ("IDEC") for using a facial analysis system that captured consumer reactions when looking at items in stores. The company was subject to penalties and was required to pay a $58,700 fine for collecting data without the consent of consumers.[18] Additional examples of bias are listed in the Risks section of this paper.

Public Sector

In many cases around the world, FRT is used by the public sector for law enforcement, public safety, and border control purposes, as well as for gaining access to digital

[18] Thiago Guimarães Moraes, Eduarda Costa Almeida, and José Renato Laranjeira de Pereira, *Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces,* AI and Ethics 1, 159-172 (2021), available at https://link.springer.com/article/10.1007/s43681-020-00014-3.

government services. Some of these uses, including use for investigations, enforcement, and prosecution, raise significant concerns around transparency, infringement of human rights, and disproportionate invasion of privacy. Some common use cases are discussed below.

Border Control - FRT is used for traveller verification at border crossings. For example, the Australian Border Force and the New Zealand Customs Service have set up an automated information processing system called Smart Gate that includes using FRT for identity verification.[19] The system compares faces of passengers to their passport photo to verify whether a traveller is who they claim to be. A similar program was installed in international airports in Canada as part of the Primary Inspection Kiosk Program.[20]

Access to services - Singapore launched the SingPass Program which gives citizens access to government and private services through a digital ID card that includes a face recognition component for identity verification purposes. The certificate allows access to banking services and tax authority services.[21]

FRT in schools - Some schools in the U.S. have implemented FRT in an attempt to improve safety, including for the prevention of school shootings.[22] In other countries,

[19] Nessa Lynch, Liz Campbell, Joe Purshouse, and Marcin Betkier, *Facial recognition technology in New Zealand*,The Law Foundation (November 2020), https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf.

[20] Matthew Braga, *Facial recognition technology is coming to Canadian airports this spring,* CBC News (March 2, 2017), https://www.cbc.ca/news/science/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344.

[21] Tim McDonald, *Singapore in world first for facial verification,* BBC News (September 25, 2020), https://www.bbc.com/news/business-54266602.

[22] Rebecca Heilweil, *Schools are using facial recognition to try to stop shootings. Here's why they should think twice,* VOX (December 20, 2019), https://www.vox.com/recode/2019/12/20/21028124/schools-facial-recognition-

such as the UK and Australia, facial recognition has been used for attendance monitoring in schools.[23] There are systems that use FRT to access e-learning systems as well.[24] Finally, there is a growing interest in facial analysis techniques to monitor student 'engagement' and learning. In Sweden, the local DPA fined an educational institution on the grounds that students' consent to this practice cannot be obtained.[25] Introducing FRT into schools is highly contentious and has been publicly criticized. According to critics, the associated invasion of privacy could harm the development of minors and create racial and neurodivergence discrimination in the face of systemic errors. For example, many students on the autism spectrum demonstrate interest or engagement differently than neurotypical students, with differences in eye contact, blinking rates, and more.[26] Moreover, the systems would also discriminate against those with physical conditions affecting facial musculature, movement, or appearance.

mass-shootings; Mack DeGeurin, *Clearview AI Says It's Bringing Facial Recognition to Schools,* Gizmodo (May 25, 2022), https://gizmodo.com/clearview-ai-facial-recognition-privacy-1848975528.

[23] Sarah Basford, *Australian Schools Have Been Trialling Facial Recognition Technology, Despite Serious Concerns About Children's Data,* Gizmodo (March 10, 2020), https://www.gizmodo.com.au/2020/03/australian-schools-trial-facial-recognition-technology-looplearn/; Cynthia O'Murchu, *Facial Recognition Cameras Arrive in UK School Canteens,* Financial Times (October 16, 2021), https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9.

[24] Mark Andrejevic & Neil Selwyn, *Facial Recognition Technology in Schools: Critical Questions and Concerns,* Learning, Media and Technology (2020), available at https://www.tandfonline.com/doi/pdf/10.1080/17439884.2020.1686014.

[25] *Facial recognition: School ID checks lead to GDPR fine,* BBC News (August 29, 2019), https://www.bbc.com/news/technology-49489154.

[26] Mark Andrejevic and Neil Selwyn, *Facial recognition technology in schools: critical questions and concerns,* Learning, Media and Technology 45:2 115-128 (2019).

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Law enforcement use[27]

Identifying a person who refuses to identify – FRT can be used to identify individuals. For example, a police officer may photograph a suspect who refuses to identify himself and compare the image using FRT located in his police vehicle with an image in other databases such as a watch-list, the Population Registrar database, Driving Licenses Database, etc.

Mugshot database – Another similar use occurs when the police arrest a suspect, collect fingerprints and a picture of the suspect, and store the picture in a database that includes pictures of suspects and detainees. Other police systems may interface with this database when the police wish to identify suspects.[28]

Investigating an offence – FRT may be used to compare an image taken from a security camera or social media with available databases, such as a mugshot database, Population Registrar, etc. Another option would be running an FRT algorithm on large amounts of digital content (such as CCTV footage) to retrospectively track the movement or actions of a suspect. The algorithm would enable police to filter the data and identify the relevant footage to track the whereabouts of the suspect.

Live FRT – Live FRT may be used to help officers locate suspects or victims in real time. In this case, live facial recognition cameras are focused on an area and, when people pass through that area, their images are streamed directly to the live FRT

[27] For a list of face recognition systems used for criminal enforcement in the EU, see the study funded by the EU, *Towards the European Level Exchange of Facial Images* (TELEFI): https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf.
[28] See for example: Edmonton Police Service, *Facial Recognition,* https://www.edmontonpolice.ca/News/FacialRec.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

system. This system would contain a 'watchlist' of wanted individuals by the police or the courts or individuals who pose a risk of harm to themselves or others. The system compares captured images to those of people on the watch list. A match between the face of a person passing by may lead to an arrest or prevention of entry to premises.

Risks

FRT use carries with it several serious risks to privacy, which triggers risk to additional human rights. The risks will vary depending on the technology and the context in which it is used. Important factors include whether the technology used is live facial recognition, facial recognition on existing or older material, or facial analysis. Any use of FRT must be carefully evaluated prior to use and continually monitored to ensure that these risks are mitigated as much as possible.

Broad Privacy Risks

The use of FRT poses severe risks to privacy, which could trigger the violation of additional rights, especially when used in public spaces or without the knowledge and consent of data subjects. Moreover, even if the data subject has given consent to the creation of a face template, the data might be abused, leaked, or used illegally or improperly. There always remains a risk of unauthorized access, for example through a breach, improper use, or even mission creep.

Public Places - FRT placed in public places (malls, public streets, etc.) captures the faces of all individuals who are passing by indiscriminately. This results in loss of

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

anonymity and the development of constant and pervasive surveillance. In addition, the use of FRT in public spaces may reveal information or allow for inferences about a person's lifestyle, including political opinion or religion (presence in demonstrations, political party's' institutions, or places of worship, wearing religious symbols or garments), medical or mental health condition (use of a wheelchair, crutches, or glasses, visiting specific clinics, etc.), sexual orientation (visiting LGBT meeting venues, etc.), and more. Additionally, in some cases, FRT or facial analysis used in public spaces may reveal traits of individuals such as age, gender, race, skin color, relationships with others, etc.

The implications of pervasive surveillance are damning for privacy in numerous ways. The fear of losing anonymity due to constant surveillance coupled with the desire to avoid documentation of movements may, in some circumstances, prevent some members of the public from attending locations where facial recognition systems are installed and consequently refrain from participating in or visiting demonstrations, gatherings, worship places, health clinics, and even train stations. This creates a chilling effect on many freedoms such as the freedom of movement, religion, speech, freedom from warrantless searches, and the right to receive health services.

Given the risks mentioned above, it should be noted that when a face recognition system is placed in the public space (or applied to recorded images or videos from regular video surveillance in the public space) in order to locate suspects or wanted individuals, the system also captures innocent individuals who are passing by and breaches their privacy when there is no public interest to do so.

Data quality and bias risks / inaccuracy and risk of error – FRT is based on probabilities and therefore errors may occur from time to time, through the different

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

components of the system. FRT has a documented history of accuracy errors, several of which perpetuate existing bias, particularly of race, gender, or neurodivergence.[29] One federal study conducted in the United States concluded that "Asian and African American people were up to 100 times more likely to be misidentified than white men."[30] In addition, certain forms of FRT, such as those purporting to act as emotion recognition or biometric characterization recognition systems, have such inherent and severe inaccuracy and bias problems that it is impossible to use them in an ethical manner. Put simply, these systems do not and cannot work.[31]

Emotion detection systems assume both universal emotional expression and a strong correlation between emotion and physical expression, though there is no evidence

[29] *See, e.g.,* Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81 (2018), 1-15; Morgan Klaus Scheuerman, Jacob M. Paul, and Jed R. Brubaker, *How Computers See Gender: an Evaluation of Gender Classification in Commercial Facial Analysis and Image Labeling Services*, Proc. ACM Hum. Comput. Interact., Vol 3, No. CSC@, Article 144 (November 2019), available at https://docs.wixstatic.com/ugd/eb2cd9_963fbde2284f4a72b33ea2ad295fa6d3.pdf; Nicholas Furl, P. Jonathon Phillips, and Alice J O'Toole, *Face recognition algorithms and the other-race effect: computational mechanisms for a developmental contact hypothesis*, Cognitive Science Vol. 26, Issue 6 (Nov-Dec 2002), 797-815; Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST, NISTIR 8280 (December 2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[30] Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, The Washington Post (December 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/, citing Patrick Grother, Mei Ngan, and Kayee Hanaoka, *supra* note 29. See also: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[31] *See* James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game,* The Verge (April 6, 2021), https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; *see also* Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, The Atlantic (April 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/; Charlotte Gifford, The Problem with Emotion-Detection Technology, The New Economy (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

that either of these exist. In fact, evidence from different cultural and social contexts demonstrates that emotional expression may vary widely across geographic, individual, and social spectrums.[32] These systems also frequently display racial bias, assigning more aggressive emotions to Black faces than White faces, regardless of actual facial expression.[33]

Biometric categorization systems similarly assume that certain biometric traits are linked to specific tendencies, inclinations, or characteristics – a premise virtually indistinguishable from phrenology or physiognomy. Companies have claimed that these systems can identify a range of traits, including sexuality, autism, likelihood of criminality, and more.[34] However, these technologies rely on historical data containing its own biases, assumptions, and prejudices, frequently exacerbating

[32] *See, e.g.,* Abeba Birhane, *The Impossibility of Automating Ambiguity*, Art. Life Vol. 27(1), 44-61.
[33] *See* Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, The Conversation (January 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404; Lauren Rhue, *Racial Influence on Automated Perceptions of Emotions*, SSRN, 1, 1 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.
[34] *See* Sally Adee, *Controversial Software Claims to Tell Your Personality From Your Face*, New Scientist (May 27, 2016), https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/; *Researchers are Using Machine Learning to Screen for Autism in Children*, Duke Pratt School of Engineering (July 11, 2019), https://pratt.duke.edu/about/news/amazon-autism-app-video; Paul Lewis, *"I was Shocked it was so Easy": Meet the Professor Who Says Facial Recognition Can Tell if You're Gay*, The Guardian (July 7, 2018), https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis; Madhi Hashemi & Margaret Hall, *Criminal Tendency Detection from Facial Images and the Gender Bias Effect*, 7 J. Big Data, 1, 1 (2020), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4#Sec9 (since retracted); Luana Pascu, *Biometric Software that Allegedly Predicts Criminals Based on Their Face Sparks Industry Controversy*, Biometric Update (May 6, 2020), https://www.biometricupdate.com/202005/biometric-software-that-allegedly-predicts-criminals-based-on-their-face-sparks-industry-controversy.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

historic and societal harms towards marginalized groups. We are yet to see evidence that these systems successfully identify anything but existing bias.

In 2022, the Privacy Commissioner of Canada made the following important observations:[35]

> "With respect to training data, one of the main considerations is the role it may play in contributing to bias in the FR system. If the training data used to generate a FR algorithm lacks sufficient representation of faces from certain demographics, the algorithm will likely produce disparate accuracy metrics across groups. It is possible for a FR algorithm to produce flawed results, particularly where it has been trained on non-representative or otherwise biased data. Studies have demonstrated considerable variation in FR algorithms with respect to the error rates they produce for faces of individuals from different racial backgrounds and across genders,[36] with other research showing that a lack of diverse and high quality training data is the main culprit.[37]
>
> Regarding the FR algorithm, there are three key considerations to be aware of with respect to accuracy. The first is that accuracy is understood *statistically*. The output of a FR algorithm is a probabilistic inference as to the likelihood

[35] OPC's (Canada) Privacy Guidance on facial recognition for police agencies, May 22, published here: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/

[36] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* Interagency Report 8280, National Institute of Standards and Technology, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[37] Jan Lunter, *Beating the bias in facial recognition technology,* Biometric Technology Today, 2020(9):5-7, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575263/

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

that two images are of the same person. It is not a verified fact about the individual. As such, accuracy is not a binary "true/false" measure, but rather is computed based on the observed error rates of the algorithm across searches. There are two types of errors to consider:

1. False positives (also known as "type I" errors) where the algorithm returns a candidate match in the face database that is not of the individual in the probe image; and
2. False negatives (also known as "type II" errors) where the algorithm fails to return a genuine match in the face database even though the database contains one.

The second consideration is that there is generally a trade-off between the false positive and false negative rate of a FR algorithm. The reason for this has to do with another component, the threshold for a probable match. Depending on how high (or low) the threshold is set, a FR algorithm will generally return fewer (or more) candidate matches. However, how many results the algorithm returns has implications on its error rates. While a higher threshold will return only higher probability candidates and lead to fewer false positives, this same threshold will in general make the algorithm more likely to miss lower probability matches and potentially lead to greater false negatives. […]

The face database and probe images are two other components that raise important issues regarding to accuracy and fairness. One consideration is the quality and/or age of the images and the effects this may have on the accuracy of the FR system. For example, studies have shown that lower quality images lead to declines in accuracy and longer time elapses between images of the

> same individual increase false negative rates.[38] However, it is also important to consider the demographics of FR images, in particular, *who* is in the face database and whether the disproportionate representation of certain groups may lead to adverse effects. A FR system may be susceptible to a "feedback loop" where the makeup of individuals in a face database leads police to repeatedly cast suspicion on them, their associates or their community, thereby increasing the disproportionality of their demographic representation over time."

A notable and persistent error is that false identifications or identification failures occur much more frequently for darker-skinned, non-binary, and transgender individuals. The consequence of such errors may be misidentification (false positive) of innocent passersby as wanted criminals or as individuals banned from entering certain premises, including education or work premises.[39] There may also be a risk of false negatives. If the police are relying on FRT with a high false negative rate, they may not achieve their objective of finding the suspect. Considering the fact that FRT captures the faces of passersby, often without their knowledge or consent, errors stigmatizing communities may result in dire consequences. When such systems are placed in public space, as discussed above, or areas with heavy traffic of data subjects

[38] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 2: Identification,* Interageny Report 8271, National Institute of Standards and Technology, September 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf

[39] Matt O'Brien, *Face recognition researcher fights Amazon over biased AI,* AP News (April 3, 2019), https://apnews.com/article/north-america-ap-top-news-artificial-intelligence-ma-state-wire-technology-24fd8e9bc6bf485c8aff1e46ebde9ec1 (A study at MIT demonstrated that, while there were extremely low error rates in Amazon's system when asked to identify genders of white men, it identified women as men in 19% of the cases and had an error rate of 31% when subjects were black women); Alex Najibi, *Racial Discrimination in Face Recognition Technology,* Harvard University (October 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

such as train stations, even a small error rate may impact a significant number of innocent individuals.

Access to Data Rights - Due to the fact that data subjects are often unaware that their data is being collected by FRT, they frequently will be unable to exercise their rights to delete, update, or access the data. Not only may they not know the processing has taken place at all, but identifying who has collected the data, what data types were collected, the processes the data may be subject to, or whom it may be shared with all becomes more difficult. The lack of knowledge and control raises the risk that the data will be transferred to various organizations and data traders without the knowledge or consent of affected individuals.

Data Security Risks

Data breaches involving data extracted from FRT may have a serious effect on data subjects. Data breaches may be the result of system hacks, unauthorized use, or improper access to data. Since a person's face is a unique and permanent feature that cannot be changed or cancelled, a biometric data breach might result in extremely serious consequences compared to breaches involving a password or credit card number, which may be changed.

In the absence of proper data security measures, hackers may use the data from FRT to steal users' identities, impersonate them, gain access to their accounts (which may include sensitive personal information), blackmail data subjects, and use their identity to carry out further illegal actions. As examples of the severity of these risks,

a massive Chinese database that included, among other items, millions of face records, was left openly exposed online for months before being taken down.[40]

Therefore data security risks increase even more when a large volume of data is being collected.

Additionally, FRT may be targeted by attack types developed specifically for those systems: Morphing Attacks and Presentation Attacks. Morphing attacks are caused by the creation of images that combine the faces of two people (e.g. a person whose entry is banned, and another person who has no such restriction). In this manner, two individuals whose faces appear in a passport or other digital certificate can gain access and passage. Presentation attacks are performed in two manners: 1) impersonating an individual whose face appears in the system (a specific person or any person whose face is included in the database) or 2) deceiving the system in order to prevent it from recognizing an intruder, which can be done by an image or a dimensional mask. Pictures of individuals which the intruder wishes to impersonate can be found on social networks.

In addition to FRT-specific attacks, more versatile attacks are possible. These may include intercepting or interfering with biometric data or extracted data and replacing it with fake data, interfering with the mechanism that compares the images for matching, replacing the face pattern with the intruders' face pattern, intercepting and

[40] Zack Whittaker, *A huge Chinese database of faces and vehicle license plates spilled online,* TechCrunch (August 30, 2022), https://techcrunch.com/2022/08/30/china-database-face-recognition/.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

destroying the output that compares the images for matching, and changing the system's decision regarding the matching or mismatch of the images.[41]

Timing Risks

Many of the risks outlines above could apply to both live facial recognition technology ("LFRT") or facial recognition used on older or existing material. However, LFRT faces additional, specific risks.[42] First, LFRT automatically collects biometric data, typically without clear justification or analysis of necessity and proportionality and without ensuring that FRT is being used for a specific purpose and that they are the appropriate method for the purpose. This approach indiscriminately processes all the collected data. Key data protection issues which can arise where LFRT is used also include the governance of these systems (including why and how they are used), transparency and data subject rights, governance of watchlists and escalation processes, and more.[43] Many uses of LFRT fall outside of data subject expectations as well, as shown by a joint investigation by Canadian DPAs in 2020. In the

[41] Raghavendra Ramachandra and Christoph Busch, *Presentation Attacks Detection Methods for Face Recognition Systems: A comprehensive Survey*, 50 ACM Computing Surveys 1 (March 2017), available at https://dl.acm.org/doi/pdf/10.1145/3038924.
[42] *See, e.g.,* Information Commissioner's Opinion, *The use of live facial recognition technology in public places,* UK Information Commissioner's Office, p. 6 (June 18, 2021), available at https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.
[43] *Id.*

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

investigated case, FRT was used in Canadian malls for the purpose of monitoring foot traffic patterns and predicting demographic information about mall visitors.[44]

Concerns about bias and abuse of these systems has prompted some companies to limit sales and/or access to FRT technology, including IBM, Amazon, and Microsoft.[45] These risks can be particularly exacerbated when combined with live facial recognition. A key example of this comes from the case of a fourteen-year-old uniformed schoolboy in London who was stopped, surrounded, taken to a side street, and questioned by plainclothes officers of the London Metropolitan Police after being mistakenly identified by the FRT.[46] Later analysis confirmed this match was non-credible and the event was criticized as a heavy-handed overreach based on an incorrect assessment.

There is also a risk of deep fakes being used to trick LFRT that uses "facial liveness verification" (a facial recognition technology feature that confirms a user is live using computer vision), as demonstrated in a research study that tested six leading

[44] *Joint investigation of The Cadillac Fairview Corporation Ltd by the Information and Privacy Commissioner of Alberta, the Privacy Commissioner of Canada, and the Information and Privacy Commissioner for British Columbia* (October 28, 2020), available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

[45] Arvind Krishna, *IBM CEO's Letter to Congress on Racial Justice Reform,* IBM (November 11, 2020), https://www.ibm.com/policy/facial-recognition-sunset-racial-justice-reforms/; *We are implementing a one-year moratorium on police use of Rekognition,* Amazon (June 10, 2020), https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition; Jeffrey Dastin and Munsif Vengattil, *Microsoft bans face-recognition sales to police as Big Tech reacts to protests,* Reuters (June 11, 2020), https://www.reuters.com/article/us-microsoft-facial-recognition-idUSKBN23I2T6.

[46] Prof. Pete Fussey and Dr. Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Human Rights Centre, University of Essex (July 2019), 124, available at https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

commercial facial liveness verification systems against the researchers' deep fakes technology.[47]

However, LFRT that does not automatically store data may have a smaller risk of database breach than systems that store templates long-term. The specifics of how these systems collect and process data, along with what databases are being used for matching, will greatly affect risk assessment in these systems.

Recommendations

There are several possible approaches to mitigating the risks posed by different FRT uses, from outright banning certain uses or systems to technical measures to universal standards. We examine these options below.

Risk Assessments and Data Protection Impact Assessment

Before starting to implement an FRT system, the first step in determining appropriate action is an honest and clear evaluation of the severity of risk of a particular FRT by the controller. This analysis must consider both use and design, as even a "good" use of FRT may be undermined by a system designed without considering privacy risks and protections, and systems designed with privacy in mind can be turned to

[47] Changjiang Li, Li Wang, Shouling Ji, Xuhong Zhang, Zhaohan Xi, Shanqing Guo, and Ting Wang, *Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era,* USENIX Security '22 (February 2022), available at https://arxiv.org/abs/2202.10673.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

improper purposes. While there may be room for additional considerations, the following elements should be part of any FRT risk assessment:

- Scope of individuals affected by the system: the more individuals whose information may be collected and otherwise processed within the FRT, the higher the overall risk

- Centralized v. de-centralized: storing the data in a centralized database poses higher risk than storing the data locally (for example, on a card or private device)

- Search engine: a system that includes a biometric database and a search engine enabling identification queries to be performed on the samples stored in the database would pose a higher risk than a system which does not include a search component.

- Live v. long-term: systems that solely match live images without automatically recording or storing footage or templates are lower risk in some ways than systems which automatically store footage or images and allow for later remote matching

- Template storage: raw data (actual image) templates pose the highest risk, while a face template stored in a manner making it difficult to restructure the original image would pose a lower risk and encoded templates pose an even lower risk

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- Method of data collection: mandatory or automatic addition of data to the system poses a higher risk, while manual addition of data to the system poses a lower risk

- Consent and transparancy: using FRT without consent and without making it transparent to the data subjects has the highest risk, while making it transparent poses a lower risk and requiring informed consent prior to the data collection would be lowest risk

- Access permissions: the higher the number of access permissions to the system, the higher the amount of risk would be (this evaluation includes any access by third-party contractors)

- Target area: installment of FRT in public or semi-public uncontrolled spaces is higher risk while installment in private and access controlled spaces is lower risk

- Considering the constant evolution of technology, the system should be regularly reassessed according to the current state of technology

Legal Requirements

There are several legal requirements that must be met when using FRT and legal approaches that could be used to address risks in FRT, varying in scope and level of restriction.

Legal Ban – Many have proposed that certain forms or contexts of FRT be wholly banned from use. These include particularly risky or harmful FRT, such as emotion

recognition or biometric categorization recognition systems, and may include broad use in public spaces.

In 2021, the European Data Protection Board and the European Data Protection Supervisor called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces as well as in other circumstances in their Joint Opinion on the AI Act proposal.[48]

In the same year, the EU Parliament set forth a resolution calling for a permanent ban on automated individual recognition in public spaces, noting that citizens should only be monitored when suspected of a crime.[49] They further called to ban use of private facial recognition databases (like Clearview AI) and predictive policing based on behavioral data. This comes on the heels of legal actions taken against Clearview

[48] https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
[49] *Use of artificial intelligence by the police: MEPs oppose mass surveillance,* European Parliament (October 6, 2021), https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

AI by DPAs in Greece,[50] the United Kingdom,[51] Sweden,[52] Germany,[53] Italy,[54] Belgium,[55] France,[56] Australia,[57] and Canada.[58]

[50] Natasha Lomas, *Selfie scraping Clearview AI hit with another €20M ban order in Europe,* TechCrunch (July 13, 2022), https://techcrunch.com/2022/07/13/clearview-greek-ban-order/.
[51] *ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted*, ICO (May 23, 2022), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.
[52] Natasha Lomas, *Sweden's data watchdog slaps police for unlawful use of Clearview AI,* TechCrunch (February 12, 2021), https://techcrunch.com/2021/02/12/swedens-data-watchdog-slaps-police-for-unlawful-use-of-clearview-ai/.
[53] *Clearview AI deemed illegal in the EU, but only partial deletion ordered,* NOYB (January 28, 2021), https://noyb.eu/en/clearview-ai-deemed-illegal-eu.
[54] *Facial recognition: Italian SA fines Clearview AI eur 20 million, bans use of biometric data and monitoring of Italian data subjects,* Garante per law Protezione dei Dati Personali (March 9, 2022), https://www.gpdp.it/home/docweb/-/docweb-display/docweb/9751323#english.
[55] Pieter Haeck, *Belgian police watchdog rules use of Clearview AI 'unlawful',* Politico (March 10, 2022), https://subscriber.politicopro.com/article/2022/03/belgian-police-watchdog-rules-use-of-clearview-ai-unlawful-00016045.
[56] *Facial recognition: the CNIL orders Clearview AI to stop reusing photographs available on the internet,* CNIL (December 16, 2021), https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.
[57] *Clearview AI breached Australians' privacy,* OAIC (November 3, 2021), https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy.
[58] Zack Whittaker, *Clearview AI ruled 'illegal' by Canadian privacy authorities,* TechCrunch (February 3, 2021), https://techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

In the United States, Vermont,[59] Maine,[60] New Hampshire,[61] Oregon,[62] and California[63] have also banned facial recognition software in different forms, as have several individual U.S. cities.[64] In 2019, over 100 organizations and several hundred experts from over 40 countries signed on to a recommendation that "countries suspend the further deployment of facial recognition technology for mass surveillance" and "establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs."[65]

Policy makers and regulators should determine clear rules for usage of FRT which may include a legal ban on certain or all usages.

Legal Basis – Another possibility is permitting use of FRT only when there is a clear, specific, and valid legal basis to do so. This will vary according to scope and location of the FRT. For example, given the high risk to privacy for FRT installed in uncontrolled areas, these systems should not be installed without preliminary public

[59] *ACLU of Vermont Statement on the Enaction of S.124, the Nation's Strongest Statewide Ban on Law Enforcement Use of Facial Recognition Technology,* ACLU (October 8, 2020), https://www.acluvt.org/en/news/aclu-vermont-statement-enactment-s124-nations-strongest-statewide-ban-law-enforcement-use.
[60] *Maine Becomes First State to Enact Statewide Ban on Face Surveillance,* EPIC (June 30, 2021), https://epic.org/maine-becomes-first-state-to-enact-statewide-ban-on-face-surveillance/.
[61] Susan Crawford, *Facial Recognition laws Are (Literally) All Over the Map,* Wired (December 16, 2019), https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.
[62] *Id.*
[63] Haley Samsel, *California Becomes Third State to Ban Facial Recognition Software in Police Body Cameras,* Security Today (October 10, 2019), https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx.
[64] Nathan Sheard and Adam Schwartz, *The Movement to Ban Government Use of Face Recognition,* EFF (May 5, 2022), https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition.
[65] *Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance Endorsements,* The Public Voice (October 2019), https://thepublicvoice.org/ban-facial-recognition/endorsement/.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

debate and a legal framework that includes principles of necessity and proportionality in place that explicitly regulates the use of FRT in the uncontrolled area.

Furthermore, in high-risk deployments such as deployments in uncontrolled areas, the organization deploying the FRT should consult the competent DPA or other competent authority prior to the deployment of the system.

It should be noted that the publication of a photograph does not automatically implicate a legal basis for the processing of the biometric data that can be extracted from that photograph.

When using FRT in public places, the system must be necessary to protect an important public interest (such as preventing serious harm in case of a circumstantiated threat to national security) that cannot be prevented by other, less invasive means. There must also be transparency and reasonable limits on location of the system, scope of its footage, and length of time that the footage will be retained and the system will be used. Where consent may be an appropriate legal basis in some circumstances, policy makers should consider when consent is infeasible or inappropriate as a basis and what other bases may be acceptable.[66] In addition, consider whether a publicly posted sign constitutes appropriate notice of the system. Where signage is an element of establishing the legal basis, it must be prominently visible before the individual enters a surveilled area, must indicate any available alternatives for accessing the space, and must clearly indicate that FRT is

[66] Consultative Committee of Council of Europe Convention 108 , Guidelines on Facial Recognition (January 28, 2021), page 7, https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

in use as opposed to a standard security camera. In addition, consider how notice will be given to those why may have difficulty reading or understanding the sign.

A clear legal basis is also required when FRT is used in access controlled spaces. The legal basis may include laws other than data protection laws, and organizations should make an analysis of what laws apply. The validity of consent as a legal basis should be assessed when no other simple alternative to facial recognition has been offered (such as entering a code, password, etc.). To the extent circumstances permit, a public authority that uses FRT will specify an alternative option for data subjects and these systems should be opt-in wherever possible.

Special attention should be given to consent about the use of FRT in cases where there is an imbalance of power between the parties, e.g workplaces, and the validity of the consent given by the data subject.

Transparency – Policy makers and regulators should determine transparency rules for controllers using FRT. Generally, the public should be notified about FRT installed in public spaces as long as the notification does not interfere with the purpose for which the system was installed when this is established by a legal basis in the public interest as necessary and proportionate in a democratic society and providing adequate safeguards.

Transparency should also include granting access to the data protection impact assessment, and to the results of any testing for accuracy or bias performed in relation to the initiative.

Data Accuracy – In order for FRT to achieve maximum reliability, conditions of the training and comparison datasets, the camera, lighting, imaging, and more must be

optimal. To ensure that FRT is not generating high error rates, controllers should determine an appropriate threshold so as to prioritize reducing certain types of error based on the nature and severity of risks, while ensuring the overall effectiveness of the FR system.[67] Additionally, there must be regular examination of the data sets used (including ensuring that the images have a range of ages, genders, skin colors, and angles; that the images were acquired legally; and that they are of sufficient quality. This can be achieved by using image quality assessment algorithm to the level of quality of images inputted into the FR system) and the error rates (both false positives and false negatives). Controllers should define the confidence score, performance metrics and performance requirements for the FRT system. If the system at some point does not meet those requirements, the controller should stop the processing until the system is upgraded and meets again the requirements. A system must be in place to regularly flag and record errors so that the system accuracy can be continuously evaluated and modified where needed – though this evaluation should include human oversight. Where FRT decisions affect data subjects (for example, by denying entry, denying service, detention, delay, etc.), the final decision must be made with human intervention (made by well- trained professionals) rather than by automated service.

Security - The use of FRT should be proportionate and relevant to the purpose of installation. Therefore, before the installation of FRT, a preliminary documented analysis must take place, per the risk assessment discussed above. The risks that should be examined are risks for the rights of data subjects, data security risks and

[67] See for example the NIST Face Recognition Vendor Test (FRVT): https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

vulnerabilities, and means to mitigate them. Additionally, before using services of sub-contractors, unique risks to FRT should be assessed.

Part of this assessment must include analysis of the technical security measures of the FRT. Appropriate data security measures should be taken and implemented to prevent unauthorized access to the data and to prevent data breaches. Authorized access to data should be restricted to the minimum required to perform their duties.

Policy makers and regulators should determine rules for minimization of data acquired by FRT. In the context of face recognition, considerations for data minimization include:

- The amount and type of personal data stored (for example, avoid storing all included images or biometric templates, and instead only store a log indicating ID number, location, and time), reducing image resolution, and erasing data about data subjects which are not matched within the system.

- Deletion of raw information such as face images (as opposed to the "face template", which is their extraction) after producing the biometric face template, if the raw information is no longer required.

- Automatic means to erase or anonymize the data after a set period of time.

- Avoid cross-referencing data with data from other sources, unless cross-referencing is strictly necessary.

- Technological means to minimize data, such as software that blurs the faces of people not targeted, irrelevant areas, etc.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- Storing the face pattern or facial extraction separately from additional data and especially identifying information.

- Encryption and anonymization of identifying data to prevent the possibility of re-identification of data subjects and to prevent the possibility of creating additional internal templates by unauthorized parties.

- Encryption of extracted data, especially when the data is stored on a centralized server, and restriction of access permissions to the encryption keys to prevent unauthorized access to the data.

- Storing data in a decentralized mode (e.g. on the user's end equipment such as a token, mobile phone, or smartphone) rather than in centralized systems.

- Limiting the period of time in which data can be used to the time necessary in order to fulfil the purpose for which the data was collected.

- Data security means to address risks to data and systems (hardware and software) throughout the data flow cycle, including the face capture and collection phase, data extraction phase, image comparison, storage, additional system decision making phase, communication channels through which information is transmitted (for example, the communication channel from the camera to a police database, a communication channel from an existing database to a third party that receives access to the information), communication encryption, and physical protection of cameras and relevant end equipment.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- Considering the adoption of standards for biometric protection such as the ISO/IEC 24745:2022[68] and the use of renewable and revocable biometric references, as well as privacy preserving biometric systems.[69]

[68] https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:24745:ed-2:v1:en
[69] See for example: https://www.esat.kuleuven.be/cosic/publications/thesis-308.pdf

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org