



BSI Standards Publication

**Facial recognition technology – Ethical
use and deployment in video
surveillance-based systems – Code
of practice**

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2024

Published by BSI Standards Limited 2024

ISBN 978 0 539 21598 4

ICS 03.100.02; 33.160; 35.080; 35.240.01

The following BSI references relate to the work on this document:

Committee reference GW/1/10

Draft for comment 23/30453500 DC

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

Contents

	Page
Foreword	III
Introduction	1
<i>Figure 1 — Facial recognition holistic process</i>	2
1 Scope	3
2 Normative references	3
3 Terms, definitions and abbreviated terms	3
3.1 Terms and definitions	3
3.2 Abbreviated terms	5
4 Principles of trustworthiness	6
4.1 General	6
<i>Figure 2 — The principles and processes to achieve the objective of trustworthiness</i>	6
4.2 Overarching principles	7
<i>Table 1 — Levels of human intervention in FRT</i>	8
5 Assessing the need	10
<i>Figure 3 — Assessing the need for FRT decision tree</i>	11
6 Development	12
6.1 Principle 1: Governance and accountability	12
6.2 Principle 2: Human agency and oversight	12
6.3 Principle 3: Privacy and data governance	12
6.4 Principle 4: Technical robustness and safety	12
6.5 Principle 5: Transparency and explainability	13
6.6 Principle 6: Diversity, non-discrimination and fairness	13
7 Procurement	13
7.1 General	13
7.2 Principle 1: Governance and accountability	14
7.3 Principle 2: Human agency and oversight	14
7.4 Principle 3: Privacy and data governance	14
7.5 Principle 4: Technical robustness and safety	14
7.6 Principle 5: Transparency and explainability	14
7.7 Principle 6: Diversity, non-discrimination and fairness	15
8 Design and installation	15
8.1 Principle 2: Human agency and oversight	15
8.2 Principle 4: Technical robustness and safety	16
8.3 Principle 5: Transparency and explainability	16
8.4 Principle 6: Diversity, non-discrimination and fairness	16
9 Operation	17
9.1 Principle 1: Governance and accountability	17
9.2 Principle 2: Human agency and oversight	18
9.3 Principle 3: Privacy and data governance	19
9.4 Principle 4: Technical robustness and safety	20
9.5 Principle 5: Transparency and explainability	21
9.6 Principle 6: Diversity, non-discrimination and fairness	21
10 Review	22
10.1 Principle 1: Governance and accountability	22
10.2 Principle 2: Human agency and oversight	22
10.3 Principle 3: Privacy and data governance	22
10.4 Principle 4: Technical robustness and safety	22
10.5 Principle 5: Transparency and explainability	22

Annex A	(informative) Reference table of policies, processes and systems	23
	<i>Table A.1 — Policies, processes and systems</i>	23
Annex B	(informative) Ethical compliance checklist	25
	<i>Table B.1 — Compliance checklist</i>	25
	Bibliography	26

Summary of pages

This document comprises a front cover, an inside front cover, pages I to IV, pages 1 to 27, and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 March 2024. It was prepared by Subcommittee GW/1/10, *Video surveillance systems (VSS), commonly known as CCTV*, under the authority of Technical Committee GW/1, *Electronic security systems and products*. A list of organizations represented on this committee can be obtained on request to the committee manager.

Information about this document

Assessed capability. Users of this British Standard are advised to consider the desirability of using components that have been demonstrated by third-party assessment to be suitable.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at knowledge.bsigroup.com, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Copyright is claimed in Figure 1. The content has been reproduced with the permission of the British Security Industry Association (BSIA). Copyright remains with BSIA. All rights reserved.

Use of this document

As a code of practice, this British Standard takes the form of recommendations and guidance. It is not to be quoted as if it were a specification. Users are expected to ensure that claims of compliance are not misleading.

Users may substitute any of the recommendations in this British Standard with practices of equivalent or better outcome. Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

It has been assumed in the preparation of this British Standard that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions of this document are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word “should” is used to express recommendations of this document. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this document. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Where words have alternative spellings, the preferred spelling of the *Shorter Oxford English Dictionary* is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations

In particular, attention is drawn to the following specific regulations:

- Employment Rights Act 1996 [\[1\]](#);
- Companies Act 2006 [\[2\]](#);
- Human Rights Act 1998 [\[3\]](#);
- Regulation of Investigatory Powers Act 2000 (RIPA) [\[4\]](#);
- Equality Act 2010 [\[5\]](#);
- Equality Act 2010 (Specific Duties) Regulations 2011 [\[6\]](#);
- Data Protection Act 2018 [\[7\]](#); and
- UK General Data Protection Regulation (UK GDPR) [\[8\]](#).

Introduction

Facial recognition technology (FRT) has been designed to improve the safety, security and wellbeing of people, as well as providing a tool to improve operational processes. FRT is one of many data analysis technologies which sit under the overarching umbrella of artificial intelligence (AI), a branch of computer science.

AI technologies perform various tasks, for example, detecting objects in images, recommending movies, examining research papers, working out trends and forecasts and writing prose. The applications for AI span across multiple sectors from healthcare to manufacturing to retail.

FRT represents a whole system approach (see [Figure 1](#)) relying upon:

- a) effective deployment of cameras;
- b) integration with facial recognition software;
- c) legitimately compiled enrolment and/or person of interest databases; and
- d) developed policies, processes and training.

FRT is used in different scenarios by a wide range of organizations across multiple sectors. It is capable of finding a face in an image and mapping the features to create a face template. This template can then be compared against other images that are stored within a database to either verify a high level of likeness (e.g. check against a passport photo; controlled environment), or identify as being present in a specific location at a particular time (e.g. a person of interest at a public event; dynamic environment) if their image is held in a general database.

Once the verification has taken place, the biometric recognition is then confirmed automatically by the FRT, or in the case of identification is passed to a human to make the decision (to confirm the recognition and either take action or do nothing), which is dependent on the specific scenario and operational requirements.

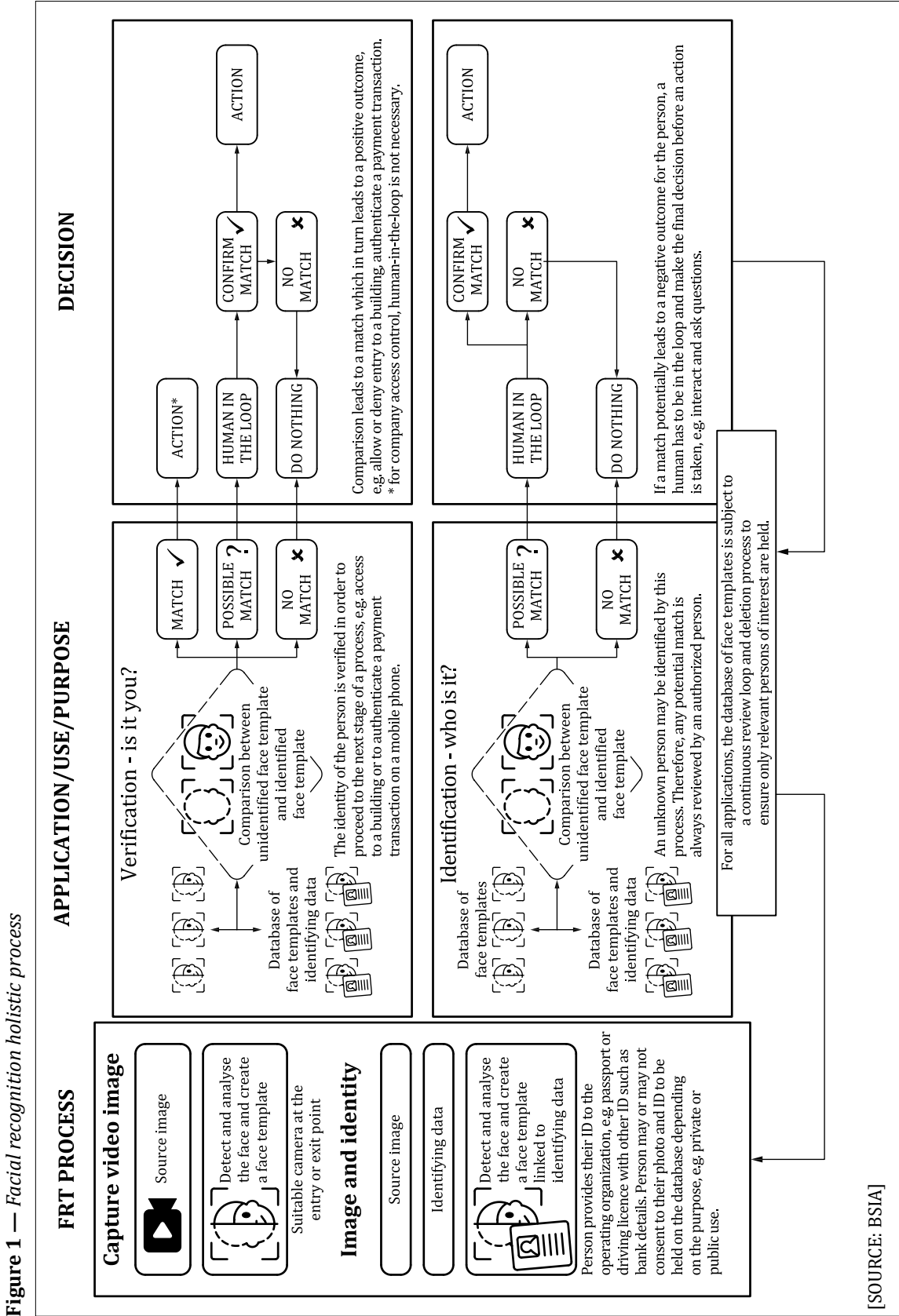
The avoidance of harm is a crucial element in the use of FRT. Harm in this sense refers to a negative impact on privacy, dignity and human rights. Human confirmation of the authentication process is an important action in instances where FRT has the potential to have a negative impact on an individual's rights.

The ethics of AI and its application, particularly FRT, need to be regularly reviewed to check that, where used for identification applications, it is not allowed to act autonomously without human oversight and is not used in any way which causes harm to individuals, in particular discrimination.

It is important that the technology within FRT is not inherently biased. It is how the AI model is trained and used which determines how accurate it is in detecting features from the widest demographic in a range of scenarios, such as different lighting levels or camera angles. An AI FRT model which is trained using facial image data which represents a wide demographic is less likely to exhibit bias by way of false positives. Bias in the AI FRT model can become magnified if the user wishes to use inaccurate reads as a means of singling out a particular demographic group.

NOTE 1 Attention is drawn to the Data Protection Act 2018 (DPA 2018) [\[7\]](#) and the UK General Data Protection Regulation (UK GDPR) [\[8\]](#).

NOTE 2 [Annex A](#) provides a summary of where policies, processes and systems are referenced in this British Standard. This is intended to assist the reader in identifying documentation necessary to each part of the supply chain involved in the deployment of an FRT system.



This British Standard is structured around six overarching principles¹⁾ which are intended to build trustworthiness among stakeholders in the use of FRT. These overarching principles are summarized in [Clause 4](#) and threaded through the provisions of each subsequent clause ([Clause 5](#) to [Clause 10](#)).

1 Scope

This British Standard provides recommendations for the ethical use and deployment of facial recognition technology (FRT) for overt, live or retrospective video surveillance purposes.

This British Standard is applicable to FRT users and system owners, as well as suppliers, integrators, maintainers and procurers, taking into account how data is captured, viewed, stored and used securely. Recommendations cover trustworthiness and the following overarching principles:

- governance and accountability;
- human agency and oversight;
- privacy and data governance;
- technical robustness and safety;
- transparency and explainability; and
- diversity, non-discrimination and fairness.

This British Standard is intended for use by public and private organizations deploying and/or monitoring FRT.

NOTE 1 Examples of users/uses include retailers, entertainment and sporting venues and private security companies deploying FRT for the purpose of crime reduction, access control, public safety, time and attendance, and monitoring authorized zones.

This British Standard excludes:

- the use of FRT in covert surveillance scenarios; and

NOTE 2 These scenarios could include those regulated by the Regulation of Investigatory Powers Act 2000 (RIPA) [4].

- domestic dwellings.

2 Normative references

There are no normative references in this document.²⁾

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1.1 artificial intelligence (AI)

engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

NOTE 1 The engineered system can use various techniques and approaches related to artificial intelligence to develop a model to represent data, knowledge, processes, etc., which can be used to conduct tasks.

NOTE 2 AI systems are designed to operate with varying levels of automation.

[SOURCE: [BS EN ISO/IEC 22989:2023](#), 3.1.4, modified]

¹⁾ Derived from <https://oecd.ai/en/ai-principles> and <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

²⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

3.1.2 biometric recognition

automated recognition of individuals based on their biological and behavioural characteristics

[SOURCE: BS EN ISO/IEC 2382-37:2023, 37.01.03]

3.1.3 data controller

entity who determines the purposes and means of processing personal data

[SOURCE: ICO's *Who does the UK GDPR apply to?* [9]]

3.1.4 data governance

setting of strategy, internal standards, integration, security, quality, data policies and practices that apply to how data is managed in accordance with law and regulations

3.1.5 data processor

entity responsible for processing personal data on behalf of a controller

[SOURCE: ICO's *Who does the UK GDPR apply to?* [9]]

3.1.6 developer

entity responsible for the design, build and delivery of an FRT product and/or service

3.1.7 ethics

set of values, principles and techniques that employ widely accepted standards of right and wrong to guide moral conduct in the development and use of AI technologies

[SOURCE: *Understanding artificial intelligence ethics and safety* [10]]

3.1.8 explainability

enables those affected (or potentially affected) by the outcome of an FRT system to understand how it was arrived at, providing those adversely affected to challenge the outcome, including the factors and logic that led to that outcome

3.1.9 face template

data corresponding to an image or images of an individual's face that is unique to that face, for use in a face recognition system

NOTE Sometimes referred to as faceprint, face map, or face signature.

3.1.10 facial recognition technology (FRT)

process by which a person can be identified or otherwise recognized from a digital facial image

[SOURCE: ICO's *The use of live facial recognition technology in public places* [11]]

3.1.11 human-in-the-loop (HITL)

systems designed to allow humans to intervene in the decision-making process of AI systems

NOTE It is accepted that HITL might not be necessary for verification applications, such as building access control, authenticating a payment transaction, or opening a phone.

3.1.12 identification

action or process of determining someone by unique biometric characteristics

3.1.13 integrator

company that either installs or integrates an FRT system

NOTE In the context of this document, a maintainer can be the same company as the integrator, or a separate company providing services to the FRT system.

3.1.14 operating organization

entity responsible and accountable for the deployment and operation of the system

3.1.15 operator

individual(s) working under the direction of the operating organization

3.1.16 profiling

categorizing an individual based on biometric characteristics, potentially leading to discrimination

3.1.17 senior accountable person (SAP)

person of seniority in the operating organization who is designated by the chief executive or managing director as having overall responsibility and accountability for strategic oversight and governance of the use of FRT

3.1.18 training data

collection of personal information used to teach a machine learning model (or FRT) to make associations or predictions between a sample of input values and output values

3.1.19 trustworthiness

ability to meet stakeholder expectations in a verifiable way

NOTE Principles of trustworthiness are further described in [Clause 4](#).

[SOURCE: [BS EN ISO/IEC 22989:2023](#), 3.5.16, modified]

3.1.20 use case

specific application in which the FRT is intended to be used

3.1.21 verification

one-to-one matching of the image of a face with the identity to verify it is the individual

[SOURCE: *Automated facial recognition: A guide to ethical use* [\[12\]](#)]

3.2 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

DPA	Data Protection Act 2018
DPIA	data protection impact assessment
FRT	facial recognition technology
GDPR	General Data Protection Regulation
HITL	human-in-the-loop
SAP	senior accountable person