SOCIETY FOR ORIGINAL BIOMETRIC IDENTITY RIGHTS · BC SOCIETY S0083123

A Standard of Consent for the Use of Biometric Identity

This standard proposes conditions under which the use of a person's voice, face, body or movement can be considered consensual. It is published by the Society as a proposal for adoption by policymakers, developers, commissioning parties and platforms, and is open to public comment. The Society does not assess or certify any entity.

ISSUING BODY
Society for Original Biometric Identity Rights

VERSION
1.0 — November 2026

© 2026 Society for Original Biometric Identity Rights

Document information

STATUS

Version 1.0, November 2026. First published version. The Society for Original Biometric Identity Rights (SOBIR) publishes this standard as a proposal for adoption and does not assess or certify any entity. Comments on this standard may be submitted at any time; details are published at sobir.ca. Correspondence: admin@sobir.ca

RELATED DOCUMENT

A Framework of Practice for the Use of Biometric Identity, published by SOBIR alongside this standard, sets out criteria of practice by which an individual or organization can meet the obligations in this standard. Where the framework and this standard differ, this standard prevails.

LICENCE

© 2026 Society for Original Biometric Identity Rights. This standard is published under the Creative Commons Attribution 4.0 International licence (CC BY 4.0), which permits sharing, adoption and adaptation, including by policymakers drafting law, provided that the Society is credited, the version is identified, any changes are indicated and no endorsement by the Society is implied. Please cite as: Society for Original Biometric Identity Rights, A Standard of Consent for the Use of Biometric Identity, Version 1.0, November 2026, sobir.ca. Adaptations: an adapted version should state: “This is an adaptation of A Standard of Consent for the Use of Biometric Identity, Version 1.0, by the Society for Original Biometric Identity Rights. Responsibility for the adaptation rests solely with its author.” Licence terms: creativecommons.org/licenses/by/4.0

Contents

Article 1	Preamble
Article 2	Scope and application
Article 3	Terms and definitions
Article 4	Consent
Article 5	Inalienable core
Article 6	Licences
Article 7	Obligations of developers
Article 8	Inquiry and demonstration of consent
Article 9	Platforms
Article 10	Exceptions
Article 11	Minors
Article 12	After death
Article 13	Recognition of compliance and legislative implementation guidance
Article 14	Adoption
Article 15	Alignment with existing law
Article 16	Review
Informative	Sources

ARTICLE 1

Preamble

1.1 Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights protect every person against arbitrary interference with their privacy and against attacks on their honour and reputation. The reproduction of a person's voice, face, body or movement without their consent engages both protections.

1.2 Generative artificial intelligence can reproduce a person's voice, face, body and movement from limited recorded material. Existing protection is largely directed at copies of recordings rather than at the person from whom they derive. In *Lehrman v. Lovo, Inc.* (S.D.N.Y. 2025), the court held that copyright does not protect a voice as such: the recordings are protected, while a synthetic voice derived from them may not be.

1.3 This standard proceeds from the principle that a person's biometric identity is an extension of their personhood. Specific uses of biometric data may be licensed; personhood itself is not transferable.

1.4 This standard is intended to support the continued development of generative technologies by establishing clear and predictable conditions for the consensual use of biometric data. Clear conditions reduce legal uncertainty for developers, commissioning parties and platforms, and protect every person, including those who build these systems.

1.5 This standard is intended for adoption by policymakers and for immediate application by developers, commissioning parties, platforms and any person or organization that uses biometric data.

ARTICLE 2

Scope and application

2.1 This standard applies to any person or organization, in any jurisdiction, that collects, uses, licenses, commissions, hosts, distributes or transfers the biometric data of another person, or that creates, uses or distributes a digital replica of another person.

2.2 This standard applies equally to every person, including those who develop, commission and operate systems that use biometric data.

2.3 Except where this standard provides otherwise, the obligations in this standard apply in proportion to the capacity of a system or use to identify, imitate or reproduce a specific person.

2.4 Nothing in this standard requires any person to act contrary to applicable law. Where law requires the processing of biometric data without consent, the processing party shall document the legal basis and limit processing to what the law requires.

2.5 Nothing in this standard limits any liability under applicable law, including liability for defamation, fraud or misrepresentation.

ARTICLE 3

Terms and definitions

3.1 In this standard, "shall" indicates a requirement, "should" indicates a recommendation and "may" indicates a permission.

3.2 Biometric data: recordings, images, scans and measurements of a person's voice, face, body or movement, at any age or stage of life, and any feature, embedding, model or output derived from them, including where altered in pitch, gender, age, language or style.

3.3 Digital replica: a computer-generated or computer-altered representation of a person's voice, face, body or movement that is readily identifiable as that person and that depicts the person saying or doing something they did not say or do, or in which the fundamental character of what they said or did has been materially altered, whether or not it is derived from that person's biometric data. Editing, restoration, remastering or format conversion of an authorized recording that does not materially alter the fundamental character of what the person said or did is not a digital replica. A person's own natural voice, face, body or movement is not a digital replica of another person, unless it is presented as, or used to impersonate, that other person.

3.4 Consent: consent given in accordance with Article 4.

3.5 Licence: a written agreement by which a person consents to a specific and limited use of their biometric data or of a digital replica of them, in accordance with Article 6.

3.6 Inalienable core: the rights set out in Article 5.1.

3.7 Commissioning party: any person or organization that requests or authorizes the use of another person's biometric data or digital replica, including a studio, agency, brand or platform.

3.8 Developer: any person or organization that collects biometric data for, or trains, builds or deploys, a system that uses biometric data or generates digital replicas.

3.9 Platform: any person or organization that hosts, stores or makes available content uploaded by others.

3.10 Chain of consent: a documented and verifiable record that identifies the sources of biometric data used and links each use of a person's biometric data to the consent that authorizes it.

3.11 Minor: a person under the age of majority in the applicable jurisdiction.

3.12 Steward: a person or body designated in writing under Article 12.

3.13 Notice: a communication submitted through the mechanism or contact point required by Article 9.9, by the person concerned or a person acting on their behalf, that identifies the content concerned and its location, states the basis of the complaint, provides contact details, and includes a statement that the information is accurate to the best of the sender's knowledge.

3.14 Commercial use: use of a digital replica in advertising, to promote or sell any product or service, or on merchandise. News reporting, commentary, criticism, scholarship or parody is not commercial use

solely because it is sold, supported by advertising or offered by subscription.

ARTICLE 4

Consent

4.1 Subject to Articles 2.4 and 10, no person shall, without the consent of the person concerned:

a. create a digital replica of that person;

b. make commercial use of a digital replica of that person;

c. distribute a digital replica of that person knowing that it was made without consent. Knowledge is established where the person distributing it has received notice, has had an upload flagged under Article 9.10, distributes a copy of content removed under Article 9.3, or where their records or statements indicate knowledge;

d. use that person's biometric data to train, build or operate any system that identifies, generates, alters or imitates human voices, faces, bodies or movement; or

e. sell, license or otherwise transfer that person's biometric data.

4.2 Consent shall be clear and conspicuous, given in writing in a separate document or a specifically signed rider, and informed by a reasonably specific description of the intended uses.

4.3 Consent to one use shall not constitute consent to any other use.

4.4 The following shall not constitute consent:

a. the public availability of recordings or images of the person;

b. ownership of a recording, or of any copyright in it;

c. a disclosure or label identifying content as synthetic;

d. an indication given under Article 9.10.

4.5 Consent shall be obtained before biometric data is collected for any purpose set out in Article 4.1. Consent obtained afterwards shall not authorize any prior use.

ARTICLE 5

Inalienable core

5.1 Notwithstanding any contract to the contrary, every person retains:

a. the right to refuse any use of their biometric data or digital replica that they have not specifically licensed;

b. the right to withdraw consent to any future use not covered by a valid licence;

c. the right to refuse any depiction of themselves in sexual content, or as endorsing any person, product or political position, unless they have consented to that specific depiction.

5.2 The rights set out in Article 5.1 shall not be transferred or waived by contract.

ARTICLE 6

Licences

6.1 A licence shall be written in clear and plain language and shall state:

a. a reasonably specific description of the intended uses;

b. the biometric data covered, including the recordings or material from which it is drawn;

c. the parties;

d. the duration;

e. the territory;

f. the payment; and

g. the conditions of termination.

6.2 Any ambiguity in a licence shall be interpreted in favour of the person whose biometric data is licensed.

6.3 The following shall not be recognized under this standard as consent to the use of biometric data:

a. terms extending to future, unspecified or "hereafter developed" technologies, media or uses;

b. terms incorporated by reference to a document not provided to the person at the time of consent;

c. general grants of rights in a performance, recording, name or likeness that do not expressly refer to biometric data or digital replicas;

d. terms that make access to an unrelated service conditional on consent to the use of biometric data;

e. terms permitting the licensee to change the scope of the licence without the person's fresh consent.

6.4 Where a commissioning party seeks a licence, it shall submit the proposed agreement, and the person shall confirm it directly before it takes effect. A licence submitted by a commissioning party without such confirmation shall not be recognized under this standard.

6.5 A valid licence binds both parties for its stated duration and within its stated terms.

6.6 The obligations under a licence and under this standard bind any successor, assignee or acquirer of the licence, of the biometric data or of any system built with it.

6.7 A licensee shall, on request, provide the person with a report of the uses made under the licence.

6.8 Upon the expiry or termination of a licence, or the withdrawal of consent where permitted under Article 5.1(b):

a. works completed before that date may continue to be used within the terms of the licence under which they were made, unless the licence provides otherwise;

b. the developer shall, expeditiously and in any event within 30 days, cease generating digital replicas of the person, cease distributing any model capable of generating them, and notify every party to whom it has supplied such a model;

c. the person's biometric data shall be excluded from the training of any subsequent version of a model;

d. where technically validated methods exist for removing a person's biometric data from an existing model, the developer shall apply them.

ARTICLE 7

Obligations of developers

7.1 A developer of a system designed or able to generate a digital replica of a specific person shall maintain a chain of consent covering every person whose biometric data was used to build the system.

7.2 A developer of any system shall take reasonable technical measures to prevent the system from generating a digital replica of a person without consent.

7.3 Where a system is found to generate a digital replica of a person without consent, the developer shall disable such generation without delay upon becoming aware of it and, on request of the person concerned, shall add that person to any mechanism it operates to block the generation of digital replicas of specific persons.

7.4 A digital replica generated by a system shall carry machine-readable provenance indicating its synthetic origin and, where applicable, the licence under which it was generated, and the developer shall take reasonable technical measures, having regard to the state of the art, to make such marking resistant to removal or alteration, including through common transformations such as re-encoding, cropping and compression, to the extent technically feasible, and shall document the measures taken. Machine-readable marking that complies with Article 50(2) of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) satisfies this requirement, provided that it also identifies any applicable licence.

7.5 A developer of a system designed or able to generate a digital replica of a specific person shall publish:

a. a summary of the sources of biometric data used to train or build the system;

b. a list of the persons of whom the system is licensed to generate digital replicas; and

c. a point of contact for inquiries under this standard.

7.6 The chain of consent shall be produced on request to the person to whom it relates, as regards that person, and to any authority with jurisdiction.

7.7 An entry in a chain of consent shall be valid only where the underlying consent complies with Articles 4 and 6. A chain of consent shall be maintained in a form capable of independent audit.

7.8 A developer of a system that generates digital replicas shall ensure that its output can be identified as generated by that system using publicly available means, and shall assist in the identification and removal of digital replicas generated by that system without consent.

7.9 A developer shall not make available a system that generates digital replicas unless it complies with Articles 7.4 and 7.8.

7.10 No person shall knowingly remove, alter or obscure the provenance marking of a digital replica.

ARTICLE 8

Inquiry and demonstration of consent

8.1 Any person may ask a developer, commissioning party or platform whether their biometric data has been used or a digital replica of them created, and shall receive a response expeditiously and in any event within 30 days. An inquiry under this article does not suspend or extend any time limit under Article 9.3.

8.2 For the purposes of this standard, where a person identifies the system, dataset or output concerned and establishes reasonable grounds that their biometric data has been used, or a digital replica of them created, without consent, the individual or organization that created or used the digital replica or biometric data, including any developer, commissioning party or uploader, shall demonstrate within 30 days, by means of the chain of consent or other written consent, that the use was authorized.

8.3 Reasonable grounds exist where any of the following is shown:

a. the person's biometric data is present in a dataset or source used by the individual or organization concerned;

b. the system or its output is named, labelled or marketed with reference to the person;

c. analysis by a generally accepted technical or forensic method, including methods published or evaluated by recognized forensic science or standards bodies, shows measurable similarity to the person's biometric data;

d. the individual or organization concerned had access to a source substantially made up of the person's biometric data;

e. the records, declarations or statements of the individual or organization concerned indicate use; or

f. the provenance marking of the digital replica concerned has been removed, altered or obscured.

8.4 Once reasonable grounds are established, the person shall not be required to demonstrate that the use was made without consent.

8.5 Where the use is not demonstrated to have been authorized within that period, the individual or organization concerned shall cease the use and remove or disable the digital replica, and any copies under its control, expeditiously and in any event within 7 days.

ARTICLE 9

Platforms

9.1 Every platform shall require, before upload, a declaration stating whether the uploader created or altered the content. Where the uploader created or altered the content, the declaration shall state whether it contains a digital replica, whose biometric data it depicts, how it was generated or altered, and whether the person depicted consented or, if not, which exception under Article 10 is relied upon. Where the uploader did not create or alter the content, the declaration shall state, to the best of the uploader's knowledge, whether it contains a digital replica and its source.

9.2 A platform shall display to viewers a clear and conspicuous indication wherever a digital replica is declared or detected.

9.3 Upon notice of a digital replica made without consent and not within an exception under Article 10, a platform shall remove or disable access to it expeditiously, and in any event within 48 hours of notice where it depicts the person in sexual content, depicts the person as endorsing any person, product or political position, or is used to defraud, and within 7 days of notice in all other cases.

9.4 A platform shall make reasonable efforts, including the use of available matching technologies, to remove or disable access to identical or substantially similar copies of content removed under Article 9.3, and to prevent their re-upload. Such efforts shall be capable of identifying copies that have been resized, re-encoded, cropped or minimally edited.

9.5 A platform shall adopt and publish a policy for the termination of users who repeatedly upload digital replicas without consent.

9.6 A person who created or altered content is deemed to know whether it contains a digital replica and whether consent was given. A knowingly false declaration under Article 9.1 shall be treated as a violation under the platform's policy under Article 9.5. A person who makes a knowingly false declaration shall not be entitled to rely on the exceptions in Article 10.

9.7 Subject to Article 9.4, nothing in this article requires a platform to monitor generally the content it hosts.

9.8 A person whose content is removed under Article 9.3 shall be notified and may submit a counter-notice, accompanied by evidence of written consent or of compliance with Article 10. The platform shall restore the content only if that evidence is satisfactory. Content removed within the 48-hour category shall remain unavailable while a counter-notice is considered. A knowingly false counter-notice shall be treated in the same manner as a knowingly false declaration under Article 9.6.

9.9 A platform shall provide an electronic mechanism for notices and counter-notices that is easy to access and use and is available without the need to create an account, and shall publish a designated contact point. A platform shall not require information beyond that set out in Article 3.13.

9.10 A notice under Article 9.3 shall allow the person concerned to indicate that they object to any digital replica of them. Where they so indicate, the platform shall, using the content removed:

a. add its titles, tags, descriptions and other metadata to its moderation filters;

b. where it operates technology for matching content or detecting digital replicas, add the person's likeness as represented in the removed content to that technology; and

c. flag for review subsequent uploads that match, and apply its policy under Article 9.5 to accounts that upload them.

9.10A The notice mechanism under Article 9.9 shall state that the platform undertakes to use biometric data held under Article 9.10 solely to detect and remove digital replicas of the person concerned and for no other purpose, including the training of any system other than for that purpose; not to transfer it to any other party, except a service provider acting solely on the platform's behalf for that purpose and

bound by the same undertakings; and to delete it expeditiously, and in any event within 30 days, if the person withdraws their indication. An indication under Article 9.10 constitutes acceptance of these undertakings, which bind the platform and any successor as an agreement with the person.

9.11 A platform shall publish, at least annually, aggregate information on notices received, digital replicas removed and accounts suspended under this article. A platform shall publish the identity of a person whose digital replicas have been removed only with that person's consent.

ARTICLE 10

Exceptions

10.1 This standard does not restrict the use of a digital replica for news reporting, commentary, criticism, scholarship or parody, provided that the use is accompanied by a clear and conspicuous disclosure, within the content itself, identifying the person depicted, stating that the depiction is synthetic and that the person did not say or do what is depicted, and that the use is not presented in a manner likely to mislead a reasonable person into believing that the person said or did something they did not say or do.

10.2 The exceptions in Article 10.1 shall be interpreted narrowly and shall not apply to:

a. sexual content;

b. depictions of the person as endorsing any person, product or political position;

c. use to defraud;

d. commercial use;

e. the training of systems intended to generate a person's likeness on demand; or

f. use in which the digital replica performs, narrates, sings or otherwise provides work that substitutes for the person's own work or performance.

ARTICLE 11

Minors

11.1 Where the person is a minor, consent under this standard shall be given by the person's parent or legal guardian, taking into account the views of the minor where the minor is capable of forming them.

11.2 No digital replica of a person who is a minor, no digital replica that depicts any person as a minor, and no biometric data collected from a person while they were a minor, shall be used in sexual content under any circumstances, whether or not consent has been given.

11.3 The exceptions in Article 10 shall not apply to digital replicas of minors.

ARTICLE 12

After death

12.1 The rights in this standard continue after the death of the person and shall be exercised by a steward designated by the person in a signed and dated writing, including a will, or, failing designation, by their estate.

12.1A A steward or estate shall exercise the rights in this standard in good faith, in accordance with the person's written directions under Article 12.2 and, where those directions are silent, consistently with the person's known wishes. A steward or estate shall not authorize any use that the person prohibited in writing.

12.1B A steward or estate shall establish its authority by the means required to administer the person's estate under applicable law, including a grant of probate or administration or its equivalent, or, where the steward is designated otherwise than by will, by a document executed with the formalities required for a will or power of attorney in the applicable jurisdiction.

12.2 A person may specify in writing, during their lifetime, the uses of their biometric data that are permitted or prohibited after their death. Such directions shall be honoured by the steward or estate for 70 years after death, and may thereafter be applied by a designated steward at its discretion.

12.3 Where no steward exists more than 70 years after death, any use of the person's biometric data shall be clearly disclosed as synthetic and shall not be presented in a manner likely to mislead.

12.4 After the death of a person, their biometric data shall not be used to depict them in sexual content, or as endorsing any person, product or political position, except as expressly permitted by a licence granted during their lifetime in accordance with Article 5.1(c), and for that licence's stated duration.

12.5 A valid licence granted during the person's lifetime continues for its stated duration.

ARTICLE 13

Recognition of compliance and legislative implementation guidance

13.1 A developer, commissioning party or platform that maintains a chain of consent in accordance with Article 7 and honours the rights set out in Article 5 should be regarded, for the purposes of this standard, as having acted in good faith.

13.2 The Society for Original Biometric Identity Rights (SOBIR) does not enforce this standard. Articles 13.3 to 13.5 identify the measures that would give effect to it where it is adopted in law or by reference.

13.3 Policymakers adopting this standard should consider making protection from liability for the use of biometric data conditional on the maintenance of a chain of consent.

13.4 Policymakers adopting this standard should provide:

- **a.** a right of action for any person whose rights under this standard are infringed;
- **b.** statutory damages, so that a person need not prove financial loss;

c. injunctive relief, including the removal of digital replicas and the disabling of models;

d. that no contract term limiting liability applies to the infringement of the rights in Article 5;

e. proportionate penalties for failure to meet the time limits in Articles 6.8, 8.1 and 9.3;

f. voluntary public registries in which a person may record the designation of a steward; and

g. protection from liability for a platform that, in good faith, removes or disables access to content in response to a notice under Article 9.

13.5 Policymakers should consider providing that a developer's failure to maintain a chain of consent in accordance with Article 7 gives rise to a rebuttable presumption that the use was made without consent.

ARTICLE 14

Adoption

14.1 This standard may be adopted by:

a. incorporation into a licence or other contract, by stating the version of this standard that governs it;

b. procurement, by requiring suppliers to demonstrate compliance with this standard;

c. platform terms, by adopting Article 9 as platform policy; or

d. reference in law, regulation or official guidance.

14.2 SOBIR publishes this standard as a proposal for adoption. SOBIR does not assess or certify any entity. Conformity may be assessed by independent bodies or by authorities designated under applicable law, including in response to a complaint by a person concerned or a member of the public. Compliance may be demonstrated to licensors, commissioning parties, insurers, platforms and authorities.

14.3 Incorporation by contract or platform terms makes this standard binding between the parties concerned. The legal effect of reference in law depends on the instrument adopting it.

ARTICLE 15

Alignment with existing law

This standard builds upon existing protections and proposes their extension:

a. Illinois' Biometric Information Privacy Act (740 ILCS 14) requires a written release before a private entity collects a person's voiceprint or scan of face geometry. This standard extends that requirement to biometric data used in artificial intelligence training in any jurisdiction.

b. California's AB 2602 (Labor Code §927) renders unenforceable contract terms that allow a digital replica of an individual's voice or likeness to be used in place of work the individual would otherwise have performed in person, where the intended uses are not reasonably specifically described and the individual was not represented by legal counsel or a labour union. This standard extends that protection from performers to all persons.

c. Quebec's Bill 24 requires consent before a person's identity or image, including audio recordings, is used in representations made to consumers. This standard extends that requirement beyond

representations made to consumers.

d. Article 50 of the EU Artificial Intelligence Act requires providers to mark synthetic audio, image and video content in a machine-readable format. Article 7.4 of this standard is compatible with that requirement and extends it to identify the licence under which a digital replica was generated.

ARTICLE 16

Review

16.1 SOBIR shall review this standard at least annually, and earlier where developments in generative artificial intelligence, biometric capture or law, or comments received, so require. Where circumstances prevent a review within that period, SOBIR shall conduct it as soon as reasonably practicable and shall publish a notice to that effect. Each version remains in effect until it is replaced. Each version shall be dated and published with a record of changes. Comments on this standard may be submitted at any time. Details are published at sobir.ca. Comments are considered at each review.

16.2 This standard was developed by SOBIR and approved by its board of directors. It is published for adoption and open public comment. Comments from any person, including experts and affected persons, are reviewed and considered at each review, and a summary of the comments received and of SOBIR's response is published with the record of changes.

INFORMATIVE

Sources

This standard draws on the following instruments. Where wording is adapted, the provisions concerned are noted.

a. Universal Declaration of Human Rights, Article 12; International Covenant on Civil and Political Rights, Article 17. Article 1.1.

b. *Lehrman v. Lovo, Inc.* (S.D.N.Y. 2025). Article 1.2.

c. California Labor Code §927 (AB 2602, 2024). Article 3.3 ("fundamental character" materially altered; editing exclusion); Articles 4.2 and 6.1(a) ("reasonably specific description"); Article 15(b).

d. California Civil Code §3344.1 (AB 1836, 2024). Article 12.2 (term of 70 years after death); Article 13.4(f) (registration of designations after death).

e. New York General Obligations Law §5-302. Articles 4.2 and 6.1(a) ("reasonably specific description").

f. Tennessee Ensuring Likeness, Voice and Image Security (ELVIS) Act (2024). Article 3.3 ("readily identifiable", whether or not derived from the person).

g. SAG-AFTRA 2023 TV/Theatrical Agreement. Article 4.2 (consent that is clear and conspicuous).

h. Illinois Biometric Information Privacy Act (740 ILCS 14). Article 4 (written consent before collection); Article 13.4(b) (damages without proof of loss); Article 15(a).

i. Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 7(2), 7(4) and 32. Articles 6.1 ("clear and plain language"), 6.3(d) (conditional consent) and 7.4 ("state of the art").

j. Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 50(2). Articles 7.4 and 15(d).

k. Regulation (EU) 2022/2065 (Digital Services Act), Article 16. Articles 3.13 and 9.9 (contents of a notice; electronic notice mechanism).

l. United States Code, Title 17, §512. Articles 9.5 (repeat-violator policy) and 9.8 (counter-notice).

m. TAKE IT DOWN Act (2025). Article 9.3 (48-hour removal); Article 13.4(g) (good-faith removal).

n. *Restatement (Third) of Unfair Competition* §47. Article 3.14.

o. Quebec, Bill 24. Article 15(c).