SOCIETY FOR ORIGINAL BIOMETRIC IDENTITY RIGHTS · BC SOCIETY S0083123

A Standard of Consent for the Use of Biometric Identity

Plain language

This is the plain language text of the Standard. It sets out, in everyday words, when the use of a person's voice, face, body or movement counts as consensual, and who is responsible for what. Where it differs from the formal text, the formal text prevails.

ISSUING BODY
Society for Original Biometric Identity Rights

VERSION
1.0, plain language — November 2026

© 2026 Society for Original Biometric Identity Rights

Document information

STATUS

Version 1.0, plain language, November 2026. This is the plain language text of the Standard. Each point is numbered to match the formal text. It is informative only and is not legal advice. Where it differs from the formal text, the formal text prevails. You can bring the Standard to a lawyer, a platform or a regulator as a clear, sourced argument for your rights. Comments may be submitted at any time; details are published at sobir.ca. Correspondence: admin@sobir.ca

RELATED DOCUMENT

The formal text of the Standard is published alongside this text, together with its sources. *A Framework of Practice for the Use of Biometric Identity*, also published by the Society for Original Biometric Identity Rights (SOBIR), sets out criteria of practice by which an individual or organization can meet the obligations in the Standard.

LICENCE

© 2026 Society for Original Biometric Identity Rights. This text is published under the Creative Commons Attribution 4.0 International licence (CC BY 4.0), which permits sharing, adoption and adaptation, 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, plain language text, November 2026, sobir.ca. Adaptations: an adapted version should state: “This is an adaptation of the plain language text 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	Why this standard exists
Article 2	Who it applies to
Article 3	Key terms
Article 4	Consent
Article 5	Rights no contract can take away
Article 6	Licences
Article 7	Developers
Article 8	Finding out, and proving consent
Article 9	Platforms
Article 10	Exceptions
Article 11	Children
Article 12	After death
Article 13	Recognition of compliance and guidance for lawmakers
Article 14	Adoption
Article 15	How this Standard builds on existing law
Article 16	Review

ARTICLE 1

Why this standard exists

1.1 Human rights treaties already protect everyone from unjustified intrusion into their privacy and from attacks on their reputation. Copying a person's voice, face, body or movement without their consent affects both.

1.2 AI can copy a person from very little recorded material. Most current protection covers recordings, not the person in them. A US court has confirmed that copyright does not protect a voice itself.

1.3 A person's identity is part of who they are. Specific uses of it can be licensed, but the person cannot be sold.

1.4 The aim is clear, predictable rules that let the technology keep developing while protecting everyone, including the people who build it.

1.5 It is written for governments to adopt and for anyone to use now.

ARTICLE 2

Who it applies to

2.1 It covers anyone, anywhere, who handles another person's biometric data or makes a digital replica of them.

2.2 It applies to everyone equally, including the people who build these systems.

2.3 The more a system can identify or copy a specific person, the more the obligations apply, unless the Standard says otherwise. A tool built to clone voices carries more duty than a general photo app.

2.4 Nobody is asked to break the law. Where the law requires something to be done without consent, whoever does it must record which law requires it and do only what that law requires.

2.5 The Standard doesn't reduce anyone's legal liability. Defamation, fraud and similar laws still apply in full.

ARTICLE 3

Key terms

3.1 "Shall" means required. "Should" means recommended. "May" means allowed.

3.2 Biometric data means recordings, images, scans and measurements of a person's voice, face, body or movement, at any age, and anything made from them, including altered versions such as a changed pitch, gender, age, language or style.

3.3 A digital replica is a computer-made or computer-altered version of a person that people would recognise as them, showing them saying or doing something they didn't, or changing what they said or did in a meaningful way, whether or not it was made from their data. Ordinary editing of a recording they agreed to, such as cleaning up sound, restoring or remastering, is not a replica as long as it doesn't change what they said or did. A person's own natural voice or face isn't a replica of someone else, unless it's used to pretend to be them.

3.4 Consent means consent given the way Article 4 requires.

3.5 A licence is a written agreement in which a person agrees to a specific, limited use of their biometric data or replica.

3.6 The inalienable core is the set of rights in Article 5 that no contract can take away.

3.7 A commissioning party is anyone who asks for or authorises the use of someone's biometric data or replica, such as a studio, agency, brand or platform.

3.8 A developer is anyone who collects data for, trains, builds or runs these systems.

3.9 A platform is any site or service that hosts content uploaded by others.

3.10 A chain of consent is the record showing where the data came from and the consent behind each use.

3.11 A minor is anyone under the age of majority where they live.

3.12 A steward is the person someone chooses, in writing, to look after their identity after they die.

3.13 A notice is a complaint sent through a platform's official channel. It says what the content is, where it is and why it's a problem, gives contact details, and confirms the information is accurate.

3.14 Commercial use means advertising, promoting or selling a product or service, or merchandise. News, commentary, criticism, scholarship and parody aren't commercial use just because they earn money.

ARTICLE 4

Consent

4.1 Unless the law requires it or an exception in Article 10 applies, nobody may do any of the following without the person's consent:

a. make a digital replica of them;

b. use a replica of them commercially;

c. share a replica of them knowing it was made without consent. A person is treated as knowing if they were sent a notice, had an upload flagged, shared a copy of something already taken down, or left records or messages showing they knew;

d. use their biometric data to train, build or run any system that recognises, generates, alters or imitates human voices, faces, bodies or movement;

e. sell, license or pass on their biometric data.

4.2 Consent must be clear and easy to see, in writing, and given in a separate document or a separately signed section. It must be based on a reasonably specific description of how the data will be used.

4.3 Agreeing to one use doesn't mean agreeing to any other use.

4.4 None of these counts as consent:

a. a person's recordings or images being publicly available;

b. someone owning a recording of the person, or the copyright in it;

c. content being labelled as AI-generated;

d. ticking the box on a takedown request asking a platform to block future clones.

4.5 Consent must be given before the data is collected. Consent given afterwards doesn't make earlier use acceptable.

ARTICLE 5

Rights no contract can take away

5.1 Whatever any contract says, every person keeps:

a. the right to refuse any use of their biometric data or replica they haven't specifically licensed;

b. the right to withdraw consent for future uses that aren't covered by a valid licence;

c. the right to refuse being shown in sexual content, or as endorsing any person, product or political position, unless they agreed to that specific depiction.

5.2 These rights can't be signed away or transferred by contract.

ARTICLE 6

Licences

6.1 A licence must be in clear, plain language and state: a reasonably specific description of the uses; exactly which data it covers, including which recordings or material; the parties; how long it lasts; where it applies; the payment; and how it can be ended.

6.2 If anything in a licence is unclear, it's read in the person's favour.

6.3 These don't count as consent:

a. terms covering future, unspecified or "yet to be invented" technologies or uses;

b. terms in another document the person wasn't given at the time;

c. general grants of rights in a performance, recording, name or likeness that don't specifically mention biometric data or replicas;

d. making an unrelated service conditional on agreeing to biometric use;

e. terms letting the licensee change what the licence covers without asking again.

6.4 If a company arranges a licence, the person must confirm it directly before it takes effect. Without that confirmation, it doesn't count.

6.5 A valid licence binds both sides for its full term and on its stated terms.

6.6 Anyone who takes over the licence, the data or a system built with it is bound by the same obligations.

6.7 On request, the licensee must give the person a report of how their data or replica has been used.

6.8 When a licence ends, is ended, or consent is withdrawn where allowed:

a. finished work can keep being used under the licence it was made under, unless the licence says otherwise;

b. as soon as possible, and within 30 days at most, the developer must stop generating replicas of the person, stop distributing models that can, and tell everyone it gave such a model to;

c. the person's data must be left out of training future versions of any model;

d. if proven methods exist to remove the person's data from an existing model, the developer must use them.

ARTICLE 7

Developers

7.1 A developer of a system built or able to replicate a specific person must keep a chain of consent covering everyone whose data was used to build it.

7.2 Developers of any system must take reasonable technical steps to stop it making replicas of people without consent.

7.3 If a system is found making replicas of someone without consent, the developer must switch that off without delay and, if asked, add the person to any block list it runs.

7.4 Replicas must carry a hidden, machine-readable marker showing they're AI-made and, where relevant, which licence covers them. Developers must make reasonable efforts to make the marker hard to remove, including surviving re-saving, cropping and compression where technically possible, and must keep records of what they did. Markers that meet the EU AI Act's rules count, provided they also identify any licence.

7.5 Developers of systems that can replicate specific people must publish a summary of where their biometric data came from, a list of the people they're licensed to replicate, and a contact for questions.

7.6 The chain of consent must be shown on request to the person it concerns (their own part of it) and to any authority with jurisdiction.

7.7 A record in the chain of consent only counts if the consent behind it meets Articles 4 and 6. The records must be kept in a form that can be checked independently.

7.8 Developers of replica tools must make sure their output can be identified as theirs using publicly available tools, and must help identify and remove replicas made without consent.

7.9 A developer may not release a replica tool unless it meets 7.4 and 7.8.

7.10 Nobody may knowingly remove, alter or hide the marker on a replica.

ARTICLE 8

Finding out, and proving consent

8.1 Anyone can ask a developer, business or platform whether their biometric data has been used or a replica of them made, and must get an answer as soon as possible, within 30 days at most. Asking never delays a takedown.

8.2 If a person points to the specific system, dataset or content and shows reasonable grounds that they were copied without consent, whoever made or used the replica or data must prove

consent in writing within 30 days.

8.3 Reasonable grounds exist if any of these is shown:

a. the person's data is in a dataset or source that was used;

b. the system or content is named, labelled or marketed using the person's identity;

c. a generally accepted technical or forensic analysis shows measurable similarity to the person;

d. whoever made it had access to a source made up mostly of the person's data;

e. their own records, declarations or statements show the data was used;

f. the hidden AI marker on the replica was removed, altered or hidden.

8.4 Once reasonable grounds are shown, the person doesn't have to prove there was no consent.

8.5 If consent isn't proven in time, whoever made or used the replica must stop and take it down, along with any copies they control, as soon as possible and within 7 days at most.

ARTICLE 9

Platforms

9.1 Before upload, platforms must ask whether the uploader made or altered the content. Creators must declare whether it contains a replica, of whom, how it was made, and whether the person consented or which exception applies. Reposters declare only what they know and where they got it.

9.2 Platforms must clearly show viewers when content contains a declared or detected replica.

9.3 When told about a replica made without consent and outside the exceptions, platforms must remove it as soon as possible: within 48 hours for sexual content, fake endorsements or scams, and within 7 days for everything else.

9.4 Platforms must make reasonable efforts, including matching technology, to remove copies and stop re-uploads, including copies that have been resized, re-saved, cropped or slightly edited.

9.5 Platforms must have and publish a policy for removing users who repeatedly upload replicas without consent.

9.6 Whoever made or altered content is treated as knowing whether it contains a replica and whether there was consent. Knowingly lying on the declaration breaks the platform's rules, and the liar loses the right to claim an exception.

9.7 Apart from blocking re-uploads, platforms aren't required to monitor everything they host.

9.8 Someone whose content is removed is told, and can challenge it with proof of consent or that an exception applies. The content only returns if the proof holds up. Sexual content, fake endorsements and scams stay down while a challenge is reviewed. Knowingly lying in a challenge has the same consequences as lying on a declaration.

9.9 Platforms must offer an easy online way to report and to challenge, with no account needed, and a published contact. They can't demand more information than the Standard lists.

9.10 When reporting a replica, a person can tick a box saying they object to any replica of them. The platform must then use the removed content (its titles, tags and other details, and any matching technology it has) to flag future uploads that match, and deal with accounts that upload them.

9.10A By offering that box, the platform promises to use the data only to catch and remove that person's replicas, never for anything else (including training other systems), never to share it except with a contractor doing that one job under the same promises, and to delete it within 30 days if the person changes their mind. Ticking the box makes that promise binding, including on anyone who takes over the platform.

9.11 Platforms must publish yearly totals of reports, removals and suspensions. They can only name a person whose replicas were removed if that person agrees.

ARTICLE 10

Exceptions

10.1 News, commentary, criticism, scholarship and parody may use a replica without consent, as long as the content itself clearly says who is shown, that it's AI-made and that they didn't say or do it, and it isn't presented in a way likely to fool a reasonable person.

10.2 These exceptions are read narrowly and never cover:

- **a.** sexual content;
- **b.** showing someone endorsing a person, product or political position;
- **c.** scams;
- **d.** commercial use;
- **e.** training systems to produce someone's likeness on demand;
- **f.** replicas that perform, narrate, sing or otherwise do work in place of the person's own work.

ARTICLE 11

Children

11.1 For anyone under 18, consent is given by their parent or legal guardian, who must take the child's own views into account where the child is old enough to form them.

11.2 Sexual content may never use a replica of a child, a replica that shows anyone as a child, or recordings or other biometric data taken from someone when they were a child. No one can consent to this.

11.3 The exceptions for news, commentary, criticism, scholarship and parody in Article 10 never apply to replicas of children.

ARTICLE 12

After death

12.1 These rights continue after a person dies. They are exercised by a steward the person named in a signed and dated document, such as a will, or, if no steward was named, by their estate.

12.1A The steward or estate must act in good faith, follow the person's written directions and, where those directions are silent, act as the person is known to have wanted. They may never allow a use the person forbade in writing.

12.1B The steward or estate proves its authority the same way an executor would under local law, such as through probate. A steward named outside a will proves it with a document signed with the same formalities as a will or power of attorney.

12.2 While alive, a person can write down which uses of their biometric data are allowed or forbidden after their death. Those directions must be followed for 70 years after death. After that, a named steward may continue to apply them.

12.3 If there is no steward more than 70 years after death, any use of the person's biometric data must be clearly labelled as AI-made and must not be presented in a misleading way.

12.4 After death, no one may use a person's biometric data to show them in sexual content or endorsing anyone or anything, unless the person specifically agreed to it in a licence while alive, and only for as long as that licence lasts.

12.5 A licence the person signed while alive stays valid for its stated length.

ARTICLE 13

Recognition of compliance and guidance for lawmakers

13.1 A developer, business or platform that keeps a chain of consent and respects people's rights under this Standard should be treated as having acted in good faith.

13.2 SOBIR does not enforce this Standard. The rest of this article sets out what lawmakers would need to do to make it enforceable.

13.3 Lawmakers adopting this Standard should consider protecting people from liability for using biometric data only if they keep a chain of consent.

13.4 Lawmakers adopting this Standard should provide:

a. the right to sue for anyone whose rights under this Standard are broken;

b. set damages, so a person does not need to prove they lost money;

c. court orders, including orders to remove replicas and to disable AI models;

d. a rule that no contract can limit liability for breaking a person's core rights in Article 5;

e. fair penalties for missing the deadlines for stopping use after a licence ends or consent is withdrawn (6.8), answering inquiries (8.1) and platform takedowns (9.3);

f. optional public registries where a person can record who their steward is; and

g. protection for platforms that remove content in good faith after a report, so they can act quickly without fear of being sued for it.

13.5 Lawmakers should consider a rule that if a developer does not keep a chain of consent, the use is presumed to have been made without consent unless the developer proves otherwise.

ARTICLE 14

Adoption

14.1 This Standard can be adopted:

a. in a licence or contract, by stating which version of the Standard applies;

b. in purchasing, by requiring suppliers to show they comply;

c. by platforms, by making Article 9 part of their policies; or

d. by referring to it in a law, regulation or official guidance.

14.2 SOBIR publishes this Standard as a proposal. SOBIR does not assess or certify anyone. Independent bodies, or authorities named by law, may check whether someone complies, including when a person or a member of the public complains. Organizations can show their compliance to the people they license from, clients, insurers, platforms and authorities.

14.3 When this Standard is written into a contract or platform terms, it is binding on the parties to it. When it is referred to in a law, its legal effect depends on that law.

ARTICLE 15

How this Standard builds on existing law

This Standard builds on protections that already exist and proposes extending them:

a. Illinois law (the Biometric Information Privacy Act) requires written permission before a business collects a person's voiceprint or face scan. This Standard extends that to AI training anywhere.

b. California law (AB 2602) makes a contract term unenforceable if it lets a digital replica of a performer's voice or likeness replace work they would have done in person, the uses are not reasonably specifically described, and the performer had no lawyer or union representing them. This Standard extends that protection to everyone.

c. Quebec law (Bill 24) requires consent before a person's identity or image, including recordings of them, is used in material presented to consumers. This Standard extends that beyond material presented to consumers.

d. The EU AI Act (Article 50) requires AI-made audio, images and video to carry a machine-readable marker. This Standard's marking rule (7.4) works with that requirement and adds that the marker must identify the licence the replica was made under.

ARTICLE 16

Review

16.1 SOBIR will review this Standard at least once a year, and sooner if technology, the law or public comments call for it. If something prevents a review on time, SOBIR will do it as soon as it reasonably can and post a notice saying so. Each version stays in force until a new one replaces it. Every version is dated and published with a record of what changed. Anyone can send comments at any time; details are at sobir.ca. Comments are considered at every review.

16.2 This Standard was developed by SOBIR and approved by its board of directors. It is published for adoption and open to public comment. Comments from anyone, including experts and people affected, are considered at every review, and a summary of the comments and SOBIR's response is published with the record of changes.