

Commercial Surveillance and Digital Likeness Protection Act (CSDLPA)

The following is a proposed fourth companion statute to accompany the Fiduciary Commons Framework's three model statutes. Unlike VIDA, PDTA, and GAAFA, this statute does not rest on the constitutional fiduciary relationship between government and citizens. It rests on legislative authority over commerce, informed by the framework's theoretical insights and enabled by the architectural infrastructure VIDA establishes. This structural separation is deliberate and essential to preserving the framework's constitutional integrity.

Section 1. Short title

This Act may be cited as the "Commercial Surveillance and Digital Likeness Protection Act."

Section 2. Legislative findings and purpose

(a) The [Legislature] finds that:

- (1) Commercial entities routinely engage in persistent, covert surveillance of individuals' online and offline activities through browser fingerprinting, cross-site tracking, location monitoring, and other techniques that operate without the individual's knowledge or meaningful consent;
- (2) This surveillance is functionally indistinguishable from conduct prohibited by stalking and surveillance statutes when performed by one individual against another, differing only in the commercial motive of the surveilling party and the surveilled individual's lack of awareness;
- (3) The compiled behavioral profiles resulting from commercial surveillance constitute digital likenesses of the surveilled individuals, rendering in data the intimate details of their daily activities, associations, health concerns, political interests, financial circumstances, and personal relationships;
- (4) The commercial value of these compiled profiles derives primarily from the surveilled individual's own behavioral output, that is, the conduct of their daily life, and not from the compiler's organizational contribution, which is limited to the structural arrangement of facts the individual generated;
- (5) The unauthorized commercial exploitation of an individual's digital likeness, constructed through covert surveillance from their own behavioral output, constitutes a dignitary harm independent of any economic injury, analogous to the harm recognized by right of publicity law when a person's likeness is commercially exploited without authorization;

(6) Existing legal frameworks, including stalking statutes, privacy laws, and consumer protection laws, do not adequately address systematic, commercially motivated surveillance conducted simultaneously against millions of individuals, because those frameworks were designed to address interpersonal targeting rather than industrial-scale data extraction; and

(7) The identity and credential infrastructure established by the Verifiable Identity and Digital Autonomy Act provides the technical means by which permission-based data practices can replace surveillance-based practices in commercial contexts.

(b) Purpose. This Act establishes protections against commercial surveillance and unauthorized construction of digital likenesses, grounded in legislative authority over commerce and the dignitary interest of individuals in controlling how their identity is commercially deployed. This Act does not derive from and does not claim the constitutional fiduciary authority that grounds VIDA, PDTA, and GAAFA. Its prohibitions and requirements are legislative policy choices, informed by the principles those statutes establish but resting on independent authority.

Section 3. Definitions

For purposes of this Act:

(a) "Commercial surveillance" means the collection, compilation, correlation, analysis, or monitoring of personal data about an identifiable individual by a non-government entity for commercial purposes, including but not limited to advertising, marketing, analytics, data brokerage, algorithmic profiling, scoring, and behavioral prediction.

(b) "Browser fingerprinting" means the collection or use of technical attributes of an individual's device, browser, or network connection, including but not limited to screen resolution, installed fonts, operating system version, browser version, language settings, timezone, canvas rendering, audio processing characteristics, and WebGL parameters, for the purpose of identifying, re-identifying, or tracking an individual across sessions, websites, or services.

(c) "Cross-site tracking" means the monitoring of an individual's activities across two or more websites, applications, or services by a single entity or network of cooperating entities, regardless of the technical mechanism employed.

(d) "Digital likeness" has the meaning established by VIDA Section 4B(a)(1).

(e) "Compiled behavioral profile" has the meaning established by VIDA Section 4B(a)(2).

(f) "Informed, specific authorization" means authorization that is:

- (i) Provided through an affirmative act by the individual, separate from any other transaction or agreement;
- (ii) Specific to the data to be collected, the purpose of collection, and the duration of collection;
- (iii) Provided after the individual has been presented, in plain language, with a description of the data to be collected, the commercial purposes for which it will be used, the entities with which it will be shared, and the commercial value, if reasonably ascertainable, that is expected to be derived;
- (iv) Revocable at any time, with revocation taking effect within [72 hours]; and
- (v) Not a condition of access to any service, product, or content. An entity may not deny, degrade, or impose additional cost on service to an individual who declines to provide authorization under this section.

(g) "Identifiable individual" means a natural person who can be identified, directly or through technically feasible re-identification, from the data collected or compiled.

Section 4. Prohibition on unauthorized commercial surveillance

(a) No entity shall engage in commercial surveillance of an identifiable individual without that individual's informed, specific authorization as defined by Section 3(f) of this Act.

(b) Browser fingerprinting conducted for the purpose of identifying, re-identifying, or tracking an individual across sessions, websites, or services is a form of commercial surveillance subject to this section. The passive or invisible nature of browser fingerprinting does not exempt it from the authorization requirement.

(c) Cross-site tracking conducted without the individual's informed, specific authorization is prohibited. Consent obtained for one website or service does not constitute authorization for tracking across other websites or services.

(d) A course of commercial surveillance, meaning persistent, repeated surveillance of an identifiable individual across two or more sessions, websites, services, or time periods, conducted without the individual's informed, specific authorization, constitutes unauthorized commercial surveillance under this Act.

(e) It is not a defense to a claim under this section that:

- (1) The individual agreed to a terms-of-service agreement, privacy policy, or other click-through instrument that purported to authorize the surveillance, unless that agreement independently satisfies the requirements of informed, specific authorization under Section 3(f);
- (2) The surveillance data was anonymized, de-identified, or aggregated, if the data can be re-identified or associated with a specific individual through any technically feasible means;
- (3) The individual's data was collected by a third-party script, advertising network, or tracking service embedded in a website or application operated by a different entity, unless the individual provided informed, specific authorization to the tracking entity; or
- (4) The surveillance was conducted for commercial rather than interpersonal purposes.

Section 5. Digital likeness protections

- (a) Every natural person holds a dignitary interest in controlling how their digital likeness is constructed and commercially deployed. This interest is grounded in the individual's autonomy and identity, not in a property right over the underlying facts.
- (b) No entity shall construct a digital likeness or compiled behavioral profile of an identifiable individual through commercial surveillance conducted without the individual's informed, specific authorization under Section 3(f) of this Act.
- (c) No entity shall commercially exploit a digital likeness or compiled behavioral profile, including through sale, license, trade, exchange, or use for advertising, marketing, analytics, scoring, pricing, or behavioral prediction, unless the individual whose behavioral output generated the profile has provided informed, specific authorization for the specific commercial use.
- (d) Duty of accounting. Any entity that derives commercial revenue from a digital likeness or compiled behavioral profile of an identifiable individual shall, upon request by that individual:
 - (1) Disclose what personal data was collected and compiled;
 - (2) Identify the commercial purposes for which the profile was used;
 - (3) Disclose the commercial revenue derived from the profile, to the extent reasonably ascertainable; and
 - (4) Identify all entities to which the profile or data derived from it was sold, licensed, or shared.

(e) An individual may, at any time, demand the deletion of any digital likeness or compiled behavioral profile constructed from their behavioral output. The entity holding the profile shall complete deletion within [30 days] of receipt of the demand, including deletion from all backup, archival, and derived datasets.

Section 6. Commercial surveillance as cognizable harm

(a) The [Legislature] hereby recognizes that unauthorized commercial surveillance and the unauthorized construction of a digital likeness constitute cognizable harms for which legal remedies are appropriate, including:

- (1) The dignitary harm of having one's identity, as rendered through the totality of one's behavioral output, commercially exploited without authorization;
- (2) The autonomy harm of being subjected to persistent covert surveillance that constrains the free exercise of associational, expressive, and decisional liberty; and
- (3) The informational harm of having intimate personal details, including health concerns, political interests, financial circumstances, religious practices, and personal relationships, compiled and commercially circulated without knowledge or consent.

(b) These harms are cognizable without proof of economic injury or emotional distress. The covert construction and commercial exploitation of an individual's digital likeness is itself the injury.

Section 7. Enforcement

(a) Private right of action. Any individual whose rights under this Act have been violated may bring a civil action against the violating entity in [court of general jurisdiction]. A prevailing plaintiff is entitled to:

- (1) Injunctive relief, including orders requiring cessation of surveillance, deletion of compiled profiles, and prohibition on future unauthorized surveillance;
- (2) Statutory damages of not less than [\$1,000] and not more than [\$10,000] per violation, or actual damages if greater;
- (3) Reasonable attorney's fees and costs; and
- (4) Any other relief the court deems appropriate.

(b) For purposes of calculating statutory damages, each individual whose data is collected through a course of unauthorized commercial surveillance constitutes a separate

violation. Each distinct commercial use of an unauthorized digital likeness constitutes a separate violation.

(c) Attorney General enforcement. The Attorney General may bring a civil action under this Act seeking injunctive relief, civil penalties of not more than [\$25,000] per violation, and any other equitable relief. The Attorney General's authority under this section is in addition to, and does not preempt, the private right of action established by subsection (a).

(d) Limitation period. An action under this section must be commenced within [three years] of the date the plaintiff discovered or reasonably should have discovered the violation.

Section 8. Relationship to existing law

(a) This Act supplements and does not preempt existing state stalking, surveillance, consumer protection, or data privacy statutes. Conduct that violates both this Act and an existing statute may be prosecuted or pursued under either or both.

(b) This Act does not create, modify, or extinguish any property right in personal data. The protections established by this Act are grounded in the dignitary interest of individuals in controlling how their identity is commercially deployed, not in ownership of the underlying facts.

(c) This Act does not impose fiduciary duties on commercial entities. The duties established by PDTA apply to entities acting in connection with government functions as defined by PDTA Section 4B(b). The obligations established by this Act arise from the legislative prohibition on unauthorized commercial surveillance, not from a fiduciary relationship.

(d) Nothing in this Act limits the authority of government entities to regulate commercial surveillance through other applicable law, including but not limited to consumer protection statutes, unfair and deceptive practices statutes, and sector-specific privacy regulations.

Section 9. Technical standards and interoperability

(a) Where an entity seeks to obtain informed, specific authorization from an individual under Section 3(f) of this Act, the entity may satisfy the authorization requirement through credential-based authorization using the identity infrastructure established by VIDA, including Verifiable Credentials, Decentralized Identifiers, and selective disclosure mechanisms.

(b) The [state agency designated under VIDA] shall publish technical guidance for commercial entities seeking to implement credential-based authorization, including specifications for interoperability with the state's VIDA-compliant identity infrastructure.

(c) An entity that implements credential-based authorization in compliance with VIDA's technical standards and the guidance published under subsection (b) is entitled to a presumption of compliance with the informed, specific authorization requirement of Section 3(f) of this Act.