Received by Legislative Council Staff
3/2/26 at 9:57 am

Be it Enacted by the People of the State of Colorado:

Single subject. This act concerns intangible personal property rights in a resident's Digital Soul and related consumer protection duties for covered operators within Colorado, including output-screening compliance (including prohibitions and duty-to-refuse controls for nonconsensual sexually explicit synthetic depictions), administrable notice, proportional remedies, emergency family or kinship tether safeguards with anti-stalking protections, payment and wallet privacy guardrails, direct-to-provider essential-support restoration mechanisms (housing, utilities, child care, health care, and transportation) with an Option B-style phased scale-up pathway that authorizes expansion of support amounts and duration up to full covered-cost payments through non-cash, direct-to-provider or direct-to-servicer rails for eligible displaced residents upon objective displacement or automation-saturation triggers and certified revenue sufficiency, with automatic pro rata scale-down upon revenue insufficiency, data minimization and separation requirements, strict retention limits, analog access pathways, explicit token parameter and audit requirements, emergency resident-directed digital repossession (freeze/cease-processing and purge directives with notice, audit logs, and due process), opt-in minors and guardianship credentialing necessary to exercise rights and access essential supports with data minimization, and a consolidated good-faith security research safe harbor that preserves existing remedies and cannot be used to evade duties; and this act shall be construed (i) as regulating in-state and Colorado-nexus commercial exploitation and identity-dependent processing of resident intangible personal property and associated deceptive practices, and not as creating an interest in land or regulating conduct wholly outside Colorado, (ii) as requiring cryptographically verifiable consent as a condition precedent to covered processing, and (iii) as authorizing restitution and

restricted wallet mechanisms only as remedial settlement and enforcement administration tools and not as a tax, debt instrument, or general entitlement.

15-15-114. Master Settlement and Sovereignty Agreement — attorney general trigger — Resident Restoration Wallet — unclaimed funds — enforcement costs.

Funding limitation; no tax authorization. The implementation of restricted wallet mechanics and the issuance of Restoration Credits referenced in this article shall be funded exclusively by: (a) lawful settlement proceeds, compliance penalties, and restitution authorized by court order; and (b) Enterprise Mitigation Revenue collected by the Automation Mitigation Enterprise pursuant to article 20 of title 24, C.R.S., if such enterprise exists and is authorized to collect and expend such revenue. If Enterprise Mitigation Revenue is unavailable for any reason, including because article 20 of title 24 is not enacted, is held invalid, or is not in effect as applied, the attorney general may administer, or contract for the administration of, restricted wallet mechanics and Restoration Credits using only the lawful settlement proceeds, compliance penalties, and restitution described in subsection (a), and the absence of Enterprise Mitigation Revenue does not delay, condition, or limit any resident right, remedy, or enforcement authority under this article. Administration of any restricted wallet mechanics under this article shall implement data minimization, purpose limitation, separation of financial rails from Digital Soul enforcement records where practicable, strict retention limits for transaction and identity verification data consistent with auditability and fraud prevention, and restricted-purpose direct-to-provider or direct-to-servicer disbursement capabilities for essential-support categories, including housing, utilities, child care, health care, and transportation, as provided in this article and by rule. Where this article authorizes an emergency freeze, cease-processing, cease-and-desist, or purge directive mechanism to prevent ongoing harm, such mechanism shall include notice, a timely opportunity to contest as established by rule, and tamper-evident audit logging sufficient for

independent review while minimizing collection of resident content. This article does not, and shall not be construed to, authorize the levy of any tax, the creation of any general welfare entitlement, or the appropriation of state General Fund moneys. Nothing in this article shall be construed to create any entitlement, property interest, or ongoing right to receive essential-support payments, Restoration Credits, or any other resident-facing financial support, and any such support is subject at all times to lawful available funding, revenue sufficiency, and the phase structure described in this article. For avoidance of doubt, any restricted wallet credit or Restoration Credit is a remedial settlement administration mechanism and not a currency, deposit account, or extension of state credit, and does not constitute state debt, and the administrator shall design payment rails to avoid unnecessary creation or retention of individualized transactional dossiers beyond what is minimum necessary for category restriction, fraud prevention, dispute resolution, audit, and unclaimed property administration. Where, and only where, objective automation-saturation or displacement triggers and phase thresholds are met, if at all, as established by rule and, where applicable, in coordination with a companion enterprise framework pursuant to article 20 of title 24, C.R.S., where enacted, the attorney general may authorize an Option B-style phased scale-up of essential-support payment amounts and duration for eligible displaced residents, up to full covered-cost direct-to-provider or direct-to-servicer payments through non-cash rails, conditioned on a contemporaneous certification of revenue sufficiency by the administering office or enterprise, as applicable, in accordance with rule. If revenue sufficiency is not certified, ceases to be certified, or funding is otherwise insufficient, the administering office shall implement an automatic pro rata scale-down of essential-support payment amounts and duration across similarly situated recipients or categories, as established by rule, to ensure expenditures do not exceed available lawful funds. Until such triggers are met

and revenue sufficiency is certified, any restricted-purpose essential-support disbursement capability under this article operates solely as a remedial restitution and settlement administration mechanism and not as a general assistance program.

(1) Legislative declaration. The general assembly finds that large-scale commercial extraction of resident Digital Soul, engagement manipulation, and automated consequential decision harms have imposed emergency damages on residents and public systems. The general assembly further finds that a standardized settlement structure is necessary to secure rapid restitution, ongoing compliance, and stable mitigation funding while reducing litigation burdens.

(2) Authorization; attorney general trigger. The attorney general is authorized to negotiate, offer, and enter into a standardized “Master Settlement and Sovereignty Agreement” (“Agreement”) with any covered commercial operator, including emergent automation operators, automated decision system operators, engagement-optimization platform operators, and consequential decision operators such as credit bureaus and tenant or employment screening entities. The attorney general may publish a standardized form Agreement and update the form as necessary to remain consistent with this article.

(3) Non-waiver. No Agreement may waive or diminish: (a) a resident’s intangible personal property rights in Digital Soul; (b) the resident’s right to revoke consent and enforce always-on veto protections; (c) any Intake Firewall obligations under this article; or (d) any emergency family or kinship tether limitations, protective-order blocks, notice, logging, or resident veto rights established by this article.

(4) Resident Restoration Wallet; in-kind remedial credit. An Agreement may establish a resident restitution mechanism known as the “Resident Restoration Wallet,” under which settlement proceeds are credited to eligible residents as a restricted-use remedial benefit to support recovery from algorithmic behavioral harms and related emergency damages. The Resident Restoration Wallet must be administered by the attorney general or, at the attorney general’s direction, by a contracted administrator, and may be coordinated with the Automation Mitigation Enterprise if it exists. The Resident Restoration Wallet:

(a) Shall pay approved merchants directly and shall not permit cash withdrawals, peer-to-peer transfers, gift card purchases, or other cash-equivalent instruments;

(b) May be used for travel, recreation, wellness, therapeutic services, housing stabilization (including rent and utilities), groceries, childcare, and other restoration categories established by rule; essential-support categories may include, as established by rule and subject to the restrictions and privacy requirements of this section, housing, utilities, child care, health care, and transportation delivered through direct-to-provider payment mechanisms; and, where authorized under the phased scale-up pathway described in subsection (4)(i), may include direct-to-servicer payments for a resident's primary-residence secured housing debt and other essential-support obligations as established by rule;

(c) Shall be designed to minimize administrative distribution costs and reduce fraud;

(d) Shall be structured to minimize tax burden to residents to the maximum extent permitted by law; however, nothing in this section purports to bind federal tax treatment; and

(e) May be used for rent, mortgage, utilities, or temporary lodging paid directly to registered housing providers, including hotels or extended-stay facilities, or to mortgage servicers and other finance companies collecting secured housing debt for a resident's primary residence, only at reasonable rates or terms established by rule where applicable and subject to audit, anti-gouging protections, and the enforcement authority of the attorney general and any applicable state consumer-protection authority; and may be used for child care, health care, and transportation only through direct-to-provider payment to verified providers and vendors as established by rule, including licensed child care providers, health care providers, pharmacies where lawful, insurers for premiums, and transit agencies or transportation providers, with category definitions, verification standards, and spend controls adopted by rule;

(f) Shall implement payment-rail privacy by design, including data minimization, purpose limitation, and the collection and retention of only the minimum transaction and identity verification data necessary to (I) prevent fraud, (II) administer category restrictions, (III) complete required audits, and (IV) comply with applicable law, and shall not require submission of resident content, communications, contact lists, device sensors, or non-payment data unrelated to payment delivery or fraud prevention;

(g) Shall, to the maximum extent practicable, maintain separation between (I) payment processing and merchant-settlement functions and (II) Digital Soul enforcement records, consent, veto, complaint, or eligibility determinations, through logical and administrative controls, so that wallet transaction data is not used for profiling, ad targeting, ranking, training, or other commercial inference about the resident;

(h) Shall provide an analog or non-digital claim and delivery pathway established by rule, including check delivery under section 15-15-116 (2), and no resident shall be required to possess a smartphone, enroll in a particular application, or submit to additional data extraction unrelated to payment delivery to receive restitution or Restoration Credits; analog access pathways shall be provided at parity of timeliness and quality; and

(i) Phased scale-up for essential-support categories; triggers; revenue sufficiency; scale-down; no entitlement. (I) The attorney general may, by rule, establish an Option B-style phased scale-up pathway under which essential-support payment amounts and duration may be expanded for eligible displaced residents upon (A) objective displacement triggers or automation-saturation triggers and phase thresholds, and (B) a contemporaneous written certification of revenue sufficiency for the applicable phase and period by the administering office or, if applicable, the Automation Mitigation Enterprise. (II) Under such phased scale-up pathway, essential-support

categories may be expanded in amount and duration up to full covered-cost payments, provided that any such payments shall be made only through non-cash rails using direct-to-provider or direct-to-servicer mechanisms with spend controls established by rule. (III) If revenue sufficiency is not certified, ceases to be certified, or available lawful funding becomes insufficient, the administrator shall implement an automatic pro rata scale-down of payment amounts and duration across similarly situated recipients or categories, as established by rule, to ensure expenditures do not exceed available lawful funds. (IV) Nothing in this subsection (4), including subsection (4)(i), shall be construed to create any entitlement, property interest, or ongoing right to receive any essential-support payment, Restoration Credit, or other benefit, and all such support remains subject to lawful available funding, the phase conditions, and the scale-down requirement; and

(j) Privacy minimization; retention limits; analog access guardrails. In administering any essential-support categories, including under the phased scale-up pathway in subsection (4)(i), the administrator shall: (I) minimize eligibility and displacement data collection to objective, minimum-necessary attributes; (II) prohibit collection or retention of resident content beyond what is strictly necessary to establish eligibility, prevent fraud, complete required audits, and deliver payments; (III) implement strict retention and deletion schedules by rule, including retention of identity verification and payment artifacts only for the minimum period necessary for audit, fraud prevention, dispute resolution, and unclaimed property administration; and (IV) ensure analog access pathways at parity of timeliness and quality, including in-person and paper submission options, and accommodation for residents without smartphones or reliable internet access. The administrator shall support an opt-in, data-minimized credentialing pathway for minors and for legal parents, court-appointed guardians, and other lawful representatives,

sufficient to (I) exercise the minor's rights under this article, (II) receive essential notices and safety alerts, and (III) administer direct-to-provider essential-support payments on behalf of a minor, while collecting only the minimum attributes necessary to verify authority and prevent fraud, using functional separation, strict retention limits, and immutable audit logs.

(5) Unclaimed restoration funds; remittance to state treasurer. Any Resident Restoration Wallet credits that remain unused or unclaimed after a dormancy period established by rule shall be treated as unclaimed property for purposes of remittance to the state treasurer. The administrator shall remit dormant balances to the state treasurer for holding and later claim by the resident under Colorado's unclaimed property procedures. Transaction records and identity verification artifacts collected solely for administration of the Resident Restoration Wallet, including records necessary to administer direct-to-provider or direct-to-servicer essential-support category payments and any phased scale-up support authorized under subsection (4)(i), shall be retained only for the minimum period established by rule necessary for audit, fraud prevention, dispute resolution, and unclaimed property administration, shall be segregated from Digital Soul enforcement records to the maximum extent practicable, and shall not be retained, sold, licensed, or repurposed for profiling, advertising, or commercial inference.

(6) Enforcement and administration costs. Any Agreement may require reimbursement to the state for reasonable costs of investigation, enforcement, expert review, audit, and administration, including necessary travel, lodging, and per diem incurred for enforcement and technical verification.

15-15-115. Intake firewall construction — ephemeral inspection — no retention without consent.

(1) Legislative declaration. The general assembly finds that technical systems must be permitted to perform minimal, transient inspection necessary to verify the presence and validity of a consent token without converting that transient inspection into "ingestion" or authorized use. This section clarifies the Intake Firewall requirements.

(2) Construction; "ingestion" means retention or downstream use. For purposes of this article, "ingestion" and "to ingest" mean storing, retaining, indexing, training upon, profiling, or otherwise using resident data beyond transient inspection strictly necessary to verify the presence and validity of a consent token or handshake; and the presence of a token does not authorize any use beyond the scope, purpose, and duration expressed in the token or handshake and this article. Any reference in this article to "48-hour" tokenized access or similar timeframes shall be construed,

unless expressly stated otherwise, as a maximum deadline for supervisory or judicial review of an access event and not as a default token validity period. Where a covered system uses rotating access tokens for access to resident-protected data, tokens must be short-lived and rotated frequently; absent a more specific rule or shorter limit, no such token may have a time-to-live exceeding fifteen (15) minutes, and refresh tokens or equivalent long-lived credentials must be rotated and reauthenticated on a schedule established by rule and in no event less frequently than every twenty-four (24) hours.

Construction; independent operability. This act is intended to be operable independently. Any cross-references to other titles or articles, including to article 20 of title 24, are for coordination only and do not require enactment of any other measure as a condition of effectiveness. If a referenced program, entity, trust, enterprise, payment rail, or mechanism (including the Automation Mitigation Enterprise, any “Trust” structure, or the “MyApp” payment rail) is not enacted, is held invalid, or is otherwise unavailable, the attorney general, the office of the digital ombudsman, and any other administering office under this act shall implement the closest administrable substitute mechanism consistent with this act, including administration through existing state platforms, paper processes, and contracted vendors, and may adopt rules as necessary to preserve resident rights, auditability, enforcement, and privacy minimization. No resident right, remedy, payment delivery, emergency freeze, cease-processing directive, purge directive, or evidence-preservation measure under this act shall be conditioned on mandatory enrollment in a particular digital wallet, application, biometric process, or ancillary data collection beyond what is strictly necessary to deliver the payment or benefit chosen by the resident or to verify legal authority for an agent acting on behalf of a minor or incapacitated resident. For the avoidance of doubt, any reference in this act to objective automation-saturation triggers or phase thresholds established under a companion enterprise framework concerns construction to avoid creation of a general welfare entitlement, and does not condition this act’s

remedies, unrestricted base restitution, or enforcement authorities on enactment of any companion measure. No provision of this act shall be construed to imply a unified subject across multiple measures or to alter the single subject stated herein.

(3) Ephemeral compliance inspection permitted. A covered system may perform transient inspection of packet headers or equivalent request metadata solely to determine whether a valid consent token or handshake is present. Such transient inspection:

(a) Must not retain content or payload; and

(b) Must not be used to train, optimize, profile, or infer about the resident.

(4) Mandatory discard; contraband classification. If a valid consent token or handshake is not present, the system shall immediately discard the request and treat any associated content or payload as contraband data subject to the prohibitions of this article, including prohibitions on retention, training, indexing, and downstream inference use.

15-15-115.5. Nonconsensual sexually explicit synthetic depiction prohibition (adult NCII) — operator duties — per se violation — emergency remedies — safe-harbor suspension.

(1) Definitions. As used in this section, unless the context otherwise requires: (a) "Nonconsensual sexually explicit synthetic depiction" means any image, video, audiovisual sequence, or other depiction, whether photorealistic or otherwise, that (I) depicts a natural person in a state of nudity or engaged in explicit sexual conduct, or depicts intimate parts as defined by rule, and (II) is generated, altered, or synthesized in whole or in part by an automated system or emergent automation system, where the depicted person did not provide a valid, active DID Handshake authorizing the creation and the specific sexually explicit use, scope, and distribution context. (b) "Generate" includes creating, rendering, inpainting, face-swapping, body-swapping, voice-swapping in connection with a sexually explicit depiction, or otherwise producing a synthetic sexually explicit depiction from any prompt, input, or reference artifact. (c) "Distribute" includes publishing, hosting, transmitting, uploading, making available for

download or viewing, embedding, sending via message, or providing access through an API, plugin, model endpoint, or other means, whether for payment or without charge.

(2) Prohibition; duty to refuse; duty to maintain effective controls. A covered operator shall not knowingly, recklessly, or negligently generate or distribute a nonconsensual sexually explicit synthetic depiction. To ensure administrable compliance, a covered operator shall: (a) Implement and maintain always-on refusal controls that prevent the generation pipeline and any hosting or distribution pipeline from completing when the operator knows or reasonably should know that the requested output is a nonconsensual sexually explicit synthetic depiction; (b) Treat any request, input, intermediate, or output artifact associated with a nonconsensual sexually explicit synthetic depiction as prohibited contraband output for purposes of retention, caching, indexing, training, and downstream inference use, regardless of whether the request included a valid DID Handshake for other purposes; and (c) Require that any DID Handshake relied upon to authorize a sexually explicit depiction be specific to (I) the depicted person, (II) the sexually explicit nature of the depiction, (III) the permitted scope of transformation, and (IV) the permitted distribution context, as established by rule; a general-purpose consent token or a token granted for non-sexual purposes does not authorize a sexually explicit depiction.

(3) Per se violation; unfair practice. The generation or distribution of any nonconsensual sexually explicit synthetic depiction is a per se violation of this article and constitutes an unlawful practice and a deceptive trade practice subject to all remedies available under this article and the Colorado Consumer Protection Act as incorporated by reference, without requiring proof of reliance, market-wide impact, or other additional elements beyond the violation.

(4) Emergency injunctive relief; mandatory suppression and preservation. Upon a sworn showing by a depicted person, the attorney general, or another authorized enforcing entity, a court shall

have authority to issue immediate temporary, preliminary, and permanent injunctive relief to stop ongoing or imminent harm, including orders requiring a covered operator to: (a) Immediately cease generation, hosting, and distribution of the nonconsensual sexually explicit synthetic depiction; (b) Implement emergency suppression controls reasonably designed to prevent materially similar re-uploads or re-generations through the operator's systems, consistent with sections 15-15-103, 15-15-106, and 15-15-119, and with rules adopted under this article; (c) Preserve non-content minimum-necessary evidence and tamper-evident audit logs sufficient for enforcement and restitution determination, while minimizing collection and retention of resident content, consistent with the Intake Firewall construction and retention limits in this article; and (d) Execute purge, de-indexing, and downstream deletion instructions to processors and vendors within the operator's contractual control to the maximum extent technically feasible, and issue a certificate of actions taken consistent with section 15-15-119.

(5) Restitution; disgorgement; damages. In addition to any other relief, a court may order restitution to the depicted person and disgorgement of any revenues, fees, or other consideration obtained in connection with the generation or distribution of the nonconsensual sexually explicit synthetic depiction, including reimbursement of reasonable costs of mitigation, safety planning, identity restoration, and therapeutic services. Nothing in this section limits statutory damages or treble damages otherwise available under this article.

(6) Safe-harbor inapplicability; suspension. Any good-faith compliance safe harbor, liability shield, limitation on remedies, or similar operator-favorable defense created by this act shall not apply to, and is proportionally suspended as to, any covered operator activity that generates or distributes a nonconsensual sexually explicit synthetic depiction. For avoidance of doubt, a

violation under this section constitutes, at minimum, reckless noncompliance for purposes of any safe-harbor analysis under this act.

(7) Compute-severance and contraband-output control mechanism; coordination and standalone fallback. For purposes of implementing the refusal, suppression, and emergency enforcement obligations in this section, a covered operator shall comply with any compute-severance, contraband-output control, account remedy, vendor exclusion, or debarment mechanism applicable to contraband outputs established in article 20 of title 24, C.R.S., where enacted and applicable. If no such mechanism is enacted, is held invalid, or is otherwise unavailable, this act remains independently operable and, as a standalone fallback, the attorney general may by rule require administrable substitute controls, including: (a) suspension or termination of the specific model endpoint, API key, account, or tenant reasonably associated with the violation, subject to notice-and-appeal where practicable and consistent with emergency prevention; (b) implementation of output suppression and hash or signature-based blocking reasonably designed to prevent re-generation or re-upload on the operator's systems; and (c) expedited preservation and production of tamper-evident audit artifacts sufficient to support injunctive relief and restitution, subject to trade-secret and privacy-minimization protections recognized by this act.

15-15-116. Resident restitution delivery — unrestricted base restitution — optional restoration credits.

(1) Legislative declaration. The general assembly finds that restitution for emergency harms must be meaningful and respect resident autonomy, including the ability to address rent, groceries, childcare, and other necessities.

(2) Unrestricted base restitution. Notwithstanding any other provision of this article, any resident restitution amount required by a Master Settlement and Sovereignty Agreement or by order of the attorney general under this article may be delivered as unrestricted legal tender via direct deposit, check, or other generally accepted payment mechanism established by rule.

(3) Optional restoration credits. In addition to unrestricted base restitution, the attorney general and, if it exists, the Automation Mitigation Enterprise (AME) may offer optional, supplemental "Restoration Credits" administered

through the Resident Restoration Wallet described in section 15-15-114. If the AME does not exist, is not in effect, or cannot lawfully administer such credits, the attorney general may administer, or contract for the administration of, Restoration Credits consistent with section 15-15-114. Use of Restoration Credits may be restricted to approved categories for restorative purposes, including essential-support categories delivered through direct-to-provider or direct-to-servicer mechanisms as authorized by section 15-15-114(4), but such restrictions shall not apply to the unrestricted base restitution under subsection (2). Administration of Restoration Credits shall be subject to the payment-rail privacy, minimization, separation, and retention-limit requirements described in section 15-15-114. Essential-support category payment amounts and duration funded through Restoration Credits shall follow the phased scale-up and automatic pro rata scale-down structure described in section 15-15-114(4)(i) where such payments are offered, including that any expansion up to full covered-cost direct-to-provider or direct-to-servicer payments through non-cash rails may occur only upon objective displacement or automation-saturation triggers and contemporaneous certification of revenue sufficiency, and shall automatically scale down pro rata if revenue sufficiency is not certified, ceases to be certified, or funding becomes insufficient. Nothing in this subsection (3) shall be construed to create an entitlement to essential-support categories or Restoration Credits.

(4) No coercion. A resident shall not be required to accept restricted-use Restoration Credits in lieu of unrestricted base restitution. A resident shall not be denied, delayed, charged a fee, or subjected to additional data extraction unrelated to payment delivery for electing to receive unrestricted base restitution under subsection (2) or for electing an analog delivery method established by rule.

15-15-119. Right to destruction and verified purge — resident-directed deletion — purge certificate.

Tiered purge and suppression. A covered operator satisfies the resident’s severance and purge directive by: (a) immediately ceasing further processing for commercial inference and suppressing future outputs that materially reproduce the resident’s Digital Soul, including by implementing an emergency freeze or cease-processing directive that is enforceable through audit logs and tamper-evident controls; (b) applying de-indexing, access controls, and suppression to cached copies and derived indices within the covered operator’s control; and (c) completing phased deletion of resident-linked records from active commercial modules within a

reasonable period where technically feasible, with a tamper-evident audit artifact documenting the actions taken. This subsection does not require unlearning of model weights where technically infeasible, provided output-phase suppression controls are implemented and verified.

(1) Right to destroy. A resident may direct a covered operator to destroy, delete, and permanently purge resident-protected data, including identifiers, profiles, embeddings, vectors, derived indices, and cached copies, to the maximum extent technically feasible, and to cease further processing of such data except as permitted under subsection (4).

(2) Scope of purge. A purge directive under this section applies to all copies of resident-protected data under the covered operator's custody or control, including data held by processors, vendors, contractors, affiliates, and downstream recipients to the extent the covered operator can lawfully compel deletion through contract, instruction, or technical control.

(3) Verification and certificate. Within a time period established by rule, a covered operator shall provide the resident a purge certificate stating:

(a) The categories of data deleted;

(b) The systems and repositories from which the data was deleted;

(c) The date and time of deletion actions; and

(d) Any limited data retained under subsection (4) and the specific statutory basis for retention.

The purge certificate shall be supported by tamper-evident logs subject to audit.

(4) Limited exceptions; legal hold. A covered operator may retain only the minimum data necessary to comply with a lawful court order, preserve evidence under a valid litigation hold, satisfy statutory recordkeeping obligations, prevent fraud or security abuse, or resolve an active dispute initiated by the resident. Any retained data must be segregated, access-controlled, and prohibited from training, profiling, targeting, ranking, or inference uses.

(5) No retaliation or service denial. A covered operator shall not deny essential service, materially degrade service quality, or impose a punitive fee solely because a resident exercised the right to destruction under this section, except where deletion makes the service technically impossible to provide without retaining the deleted data.

(6) Enforcement. A failure to honor a valid purge directive constitutes a deceptive trade practice and an unfair practice subject to all remedies available under this article and the Colorado Consumer Protection Act as incorporated by reference.

15-15-120. Death purge directive — executor authority — default purge rule — limited holds.

(1) Death purge option. A resident may, at any time, file a “death purge directive” as part of the resident’s digital deed or by separate instrument, directing covered operators to destroy and permanently purge resident-protected data upon verified notice of the resident’s death.

(2) Default rule; election required. The default post-mortem status is governed by the resident’s digital deed and probate administration. If the resident has elected death purge by directive, death purge applies notwithstanding other post-mortem provisions, except as limited by subsection (5) and section 15-15-121 (Family vault and heritage archive).

(3) Verification of death; executor notice. A covered operator shall implement a reasonable process to verify death notice, which may include submission of a death certificate, court letters testamentary, small-estate affidavit, or other proof established by rule. The resident’s personal representative, executor, or administrator may submit and enforce the death purge directive on behalf of the estate.

(4) Scope; downstream purge. Upon verified notice under subsection (3), the covered operator shall initiate purge consistent with section 15-15-119, including reasonable downstream deletion instructions to processors, vendors, contractors, affiliates, and recipients under the covered operator’s control.

(5) Limited exceptions. A covered operator may retain only the minimum data necessary to:

(a) Comply with a lawful court order;

(b) Preserve evidence under a valid litigation hold;

(c) Satisfy statutory recordkeeping obligations; or

(d) Resolve an active dispute involving the estate.

Any retained data must be segregated, access-controlled, and prohibited from training, profiling, targeting, ranking, or inference uses.

(6) Purge certificate to estate. The covered operator shall issue a purge certificate to the personal representative confirming completion of purge actions and identifying any limited data retained under subsection (5) with the specific statutory basis for retention.

(7) Enforcement. Failure to honor a valid death purge directive constitutes a deceptive trade practice and an unfair practice subject to all remedies available under this article and the Colorado Consumer Protection Act as incorporated by reference.

15-15-121. Family vault and heritage archive — post-mortem preservation election — successor access keys.

(1) Purpose. The general assembly finds that certain information has enduring family, medical, genealogical, historical, and cultural value that should not be involuntarily erased by automated deletion. This section authorizes a resident to preserve a limited set of "heritage records" in an encrypted family vault while still purging commercial and behavioral extraction data.

(2) Election by resident. A resident may, in the resident's digital deed, designate a "family vault election" identifying categories of heritage records to be preserved post-mortem and the persons authorized to access such records ("successor beneficiaries"). A family election may be used together with, or in addition to, a death purge directive.

(3) Heritage records defined. "Heritage records" means only the following categories as elected by the resident:

(a) Medical and health records necessary for family medical history, including immunization history and clinically relevant diagnoses, excluding third-party marketing profiles;

(b) Genealogical records, family photographs and videos, letters, journals, and similar personal archives;

(c) Legal and estate records necessary for probate administration; and

(d) Other categories approved by rule that are narrowly tailored to family history preservation and do not re-create a commercial behavioral profile.

(4) Encrypted vault; segregated storage. A covered operator that maintains heritage records pursuant to a family vault election shall:

(a) Segregate heritage records from commercial profiles, advertising identifiers, embeddings, targeting data, and behavioral extraction datasets;

(b) Store heritage records encrypted at rest with access governed by successor keys; and

(c) Prohibit use of heritage records for advertising, ranking, targeting, training, profiling, or inference unrelated to vault preservation.

(5) Successor access; key control. Access to heritage records shall be granted only to successor beneficiaries designated by the resident or the resident's personal representative acting pursuant to the digital deed and probate administration. The covered operator shall implement a reasonable successor verification process established by rule. No facility staff, operator personnel, or vendor may access vault content absent the successor's authorization, except as required for cybersecurity integrity and without human review of content.

(6) with death purge. If a resident has elected death purge under section 15-15-120 and also elected a family vault under this section, the covered operator shall execute death purge for all resident-protected data other than the elected heritage records retained in the family vault. Any retention beyond elected heritage records is prohibited unless authorized under section 15-15-120 (5).

(7) Patient access and HIPAA parity; ownership neutral. Nothing in this section or this article limits, diminishes, or delays a patient's right to access, inspect, obtain copies of, or direct the transmission of the patient's medical or health information as authorized by applicable state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations. This article is intended to be ownership-neutral as to medical institutions' recordkeeping interests while ensuring the resident retains read, share, and portability rights over the resident's medical information.

(8) Post-mortem medical history as heritage record. Where a resident elects to preserve medical and health records as "heritage records" under subsection (3)(a), successor beneficiaries designated by the resident may access only the preserved categories for family medical history purposes, subject to reasonable verification and any applicable HIPAA personal representative rules and probate administration. Preserved heritage records may not be used for marketing, profiling, training, or commercial inference.

15-15-122. Legacy tracking technologies — cookies, pixels, beacons, and fingerprinting — parity and default-off rules — legacy purge.

(1) Definitions. As used in this section:

(a) "Legacy tracking technology" means any cookie, third-party cookie, tracking pixel, web beacon, SDK beacon,

device fingerprinting method, cross-device identifier, advertising identifier, probabilistic identifier, or other mechanism used to observe, infer, or persistently identify a resident across sessions, sites, applications, or devices.

(b) "Reject parity" means that rejecting or declining tracking must be as easy, prominent, and functional as accepting tracking, and must not materially degrade nonoptional service beyond what is technically necessary.

(2) Default-off; opt-in required. A covered operator shall not deploy or honor a legacy tracking technology for a resident unless the resident has affirmatively opted in through a consent interface that complies with this article. Silence, continued use, pre-checked boxes, bundled consent, or ambiguous design does not constitute opt-in.

(3) Reject parity and no dark patterns. Any consent interface for legacy tracking technology must provide reject parity and must not use dark patterns, deceptive design, or coercive choice architecture. A covered operator shall not:

(a) Make "accept" more prominent than "reject";

(b) Require multiple steps to reject than to accept;

(c) Reset a resident's tracking choice more frequently than required for security; or

(d) Condition essential service on consenting to legacy tracking technology, except where the tracking is strictly necessary to provide the specific requested functionality.

(4) Read-only handshake; no tracking on reject. When a resident declines tracking, the covered operator may process a minimal "read-only" session handshake strictly necessary for security, fraud prevention, load balancing, or basic session continuity, but shall not use the handshake to build profiles, perform cross-context behavioral advertising, train models, or create persistent identifiers.

(5) Legacy purge and retrofit. Legacy tracking data and identifiers collected without valid opt-in under this article shall be treated as unverified resident-pro data. A covered operator shall:

(a) Within a time period established by rule, either obtain a compliant opt-in for continued retention and use, or permanently purge such legacy tracking data under section 15-15-119; and

(b) Ensure that processors, vendors, and downstream recipients under the operator's contractual control receive purge instructions consistent with subsection (5)(a).

(6) Enforcement. A violation of this constitutes a deceptive trade practice and an unfair practice subject to all remedies available under this article and the Colorado Consumer Protection Act as incorporated by reference.

BILL 1: THE PERSONAL DATA AND DIGITAL PROPERTY RIGHTS ACT

STATE OF COLORADO

BILL 1

A Bill for an Act Concerning the Establishment of Digital Property Rights for the Residents of the State of Colorado.

SECTION 1. In Colorado Revised Statutes, add article 15 to title 15 as follows:

ARTICLE 15

PERSONAL DATA AND DIGITAL PROPERTY RIGHTS

PART 1

GENERAL PROVISIONS

15-15-100. Short title.

This article shall be known and may be cited as the “Personal Data and Digital Property Rights Act of 2026.”

15-15-100.5. Legislative declaration.

EMERGENCY FINDINGS. The general assembly finds and declares that the rapid deployment of artificial intelligence and automated systems constitutes an ongoing emergency affecting the public peace, health, safety, and welfare because (a) a single image, voice sample, or behavioral trace can be used to generate nonconsensual synthetic likeness outputs, including sexually explicit depictions, coerced performances, and impersonations, at population scale and at near-zero marginal cost; (b) such outputs are rapidly replicable and effectively irreversible once distributed, rendering traditional takedown and post hoc remedies inadequate; Existing civil and criminal remedies addressing harassment, fraud, or nonconsensual intimate imagery are insufficient to prevent or remedy these harms in real time because they lack a standardized, machine-verifiable consent and revocation mechanism at the point of ingestion and use, and because synthetic outputs can be replicated across platforms faster than enforcement can occur. (c) unlawful ingestion of resident data (“contraband data”) and high-speed model replication can compound harms before a resident can obtain relief; and (d) an enforceable, standardized mechanism to verify resident ownership and consent—through Digital Soul title, cryptographic Handshake, and intake-gate controls—is necessary for immediate prevention of future use and for accountable remedies when violations occur.

(1) The general assembly hereby finds and declares that:

(a) The biological and behavioral data of Colorado residents constitutes a form of inalienable intangible personal property, the extraction and commercial use of which demands enforceable rights of control, exclusion, revocable licensing, and remedies consistent with constitutional limits;

(b) Existing federal and state privacy frameworks are insufficient to protect residents from the unconsented extraction, replication, and commercial exploitation of their digital lives by automated systems and artificial intelligence;

(c) The establishment of enforceable intangible personal property rights in personal data, coupled with mandatory consent mechanisms and hardware-level protections, is necessary to preserve the economic sovereignty and constitutional rights of Colorado residents; and

(d) It is the intent of the people of the state of Colorado to codify the “Digital Soul” as intangible personal property of the resident (and not real property), to guarantee the right of revocable consent, and to ensure that no entity may derive commercial benefit from a resident’s data without a valid, cryptographically verifiable authorization.

(e) Construction; constitutional nexus. Nothing in this article creates an interest in land or real property, and nothing in this article regulates conduct occurring wholly outside Colorado absent a sufficient Colorado nexus, including commercial delivery to or targeting of a Colorado resident or deployment of covered systems in Colorado.

Authority and construction map (nonexclusive). This article shall be construed and, where relevant, defended as follows: (1) Property-right framing (intangible personal property; not land): grounded in the State's traditional authority to define and protect property interests and to provide civil remedies for misappropriation and conversion-like harms, including through consumer-protection and unfair-practice prohibitions; the Act expressly disclaims creation of any

interest in real property. (2) Consent and token gating (Handshake/Intake Firewall): grounded in the State's police powers to prevent deception, misappropriation, and identity-dependent exploitation, and to require minimum necessary verification controls as a condition of lawful commercial processing directed at Colorado residents. (3) Restitution and wallet structure (remedial administration; no entitlement; no tax): grounded in settlement and restitution administration authority, with express limitations that prevent characterization as a tax, state debt, or general welfare entitlement, and with resident election and unrestricted base restitution preserved. (4) Privacy minimization, retention limits, and analog access parity: grounded in consumer protection, due process, and accessibility principles by requiring minimum-necessary collection, functional separation, strict retention limits, and meaningful non-digital pathways for notice, election, and delivery. (5) Severability and independent operability: grounded in legislative severability doctrine and the stated intent that the Act remain operative notwithstanding non-enactment, invalidation, or unavailability of any companion enterprise, trust, or payment rail, with administrable substitute mechanisms authorized to preserve resident rights and enforcement.

DEFINITIONS

15-15-100.7. Definitions.

As used in this article, unless the context otherwise requires:

(1) “Analog Sanctuary” means a physical space designated under this article where no automated data collection, biometric scanning, or algorithmic surveillance is permitted, and where essential government and commercial services must be available through non-digital means.

(2) “Compute Parity” means the standard requiring that algorithmic decision-making systems achieve no less than ninety percent (90%) accuracy and fairness when measured against equivalent human decision-making benchmarks.

(3) “Contraband Data” means any data ingested, processed, or stored without a valid DID Handshake or in violation of the Intake Firewall established under section 15-15-106, including but not limited to covert audio capture, unconsented biometrics, and shadow profiles.

(4) “DID Handshake” or “Handshake” means a mutual cryptographic verification session utilizing a Decentralized Identifier (DID) granted by a resident to a specific entity for a specific purpose and limited duration, serving as the sole valid mechanism for consent to data extraction.

(5) “Digital Deed” or “Master Deed” means the legal instrument, issued and recorded by the state of Colorado, granting a resident ultimate write-authority and exclusive licensing control over their Digital Soul, digital likeness, and all data derived therefrom.

(6) “Digital Soul” means the inseparable nature of the biological and behavioral data attributable to a natural person, including biological data hashes, behavioral data, biometric identifiers, digital likeness, and machine-readable patterns, held by the resident as intangible personal property, together with the rights to control, exclude, license, alienate, and direct deletion of such data as provided in this article.

(7) “Dopamine Ceiling” means the behavioral safety threshold established under section 15-15-108 to prevent addictive engagement-design patterns.

(8) “Hash Sentinel” means the real-time notification and veto system established under section 15-15-103 that detects and reports attempts to generate, replicate, or derive a resident’s biometric hash without authorization.

(9) “Inpainting Solution” means the technical process by which a platform or content creator replaces or removes a resident’s likeness from generated content within the timeframe mandated by section 15-15-102.

(10) “Intake Firewall” means the mandatory software-level gate established under section 15-15-106 that automatically rejects Contraband Data at the interface level prior to ingestion.

(11) “Touch” or “Ingest” means any algorithmic process that collects, stores, analyzes, trains upon, performs inference with, or modifies data derived from a human subject, including but not

limited to model training, real-time inference, and biometric scanning.

(12) “Zero-Knowledge Relay” means a cryptographic protocol that allows verification of a resident’s consent status without revealing any identifying information about the resident to the querying entity.

(13) “Covered operator” means any person or business entity that, for commercial benefit, operates, deploys, offers, sells, licenses, or provides a covered system or data-processing service to or directed at a Colorado resident, or otherwise processes resident-protected data, and includes the person that retains operational control over such activity through authority, license, or delegation.

(14) Delegated system; operator responsibility. Any automated system, model, tool, contractor, processor, or service operating under the authority, license, or delegation of a covered operator is deemed an extension of that operator for purposes of duties, remedies, and liability under this article, regardless of subcontracting or vendor arrangements.

DIGITAL PROPERTY RIGHTS

15-15-101. Digital Deed — Title and Intangible Personal Property Rights in Digital Soul.

(1) Every natural person who is a resident of the state of Colorado holds title to their Digital Soul as intangible personal property. This property right is inalienable and shall not be waived, assigned, or extinguished by contract, terms of service, or operation of law, except as expressly authorized by this article for limited licensing.

(2) The state of Colorado, through the myColorado digital platform or its successor, shall issue a Digital Deed to each resident upon request or upon attaining the age of majority. The Digital Deed shall serve as the legal instrument of record evidencing the resident’s superior title to their Digital Soul.

(3) The Digital Deed shall grant the holder exclusive write-authority over all data packets derived from or attributable to the holder, including biometric hashes, behavioral profiles, inference outputs, and likeness derivatives.

(4) A Digital Deed shall be inheritable and subject to probate proceedings under title 15. A youth multiplier of one and one-half (1.5x) shall apply to the assessed value of a minor's Digital Soul for purposes of probate and fiduciary accounting.

(5) No entity shall touch or ingest any component of a resident's Digital Soul without a valid, active DID Handshake. Any data obtained in violation of this subsection shall be classified as Contraband Data. Violations of this property right are subject to private civil action and statutory damages.

15-15-102. Mandatory Disconnection Protocol — Revocable Consent.

(1) Every resident shall have the absolute right to revoke consent for the use of their Digital Soul at any time, for any reason, without penalty. Consent granted via a DID Handshake shall be revocable in whole or in part.

(2) Upon revocation of consent, the receiving entity shall:

(a) Cease all touching and ingestion of the resident's Digital Soul within twenty-four (24) hours of receiving notice of revocation;

(b) Complete a full purge of all stored data derived from the resident's Digital Soul within seventy-two (72) hours, verified by a zero-knowledge cryptographic proof of deletion; provided that, within twenty-four (24) hours of receiving a revocation and purge directive, a covered operator may provide written notice asserting one or more of the following: (I) an active dispute initiated by the resident is pending; (II) a lawful litigation hold obligation applies to the specific data; or (III) the data is not "resident-protected data" as defined in this article; in which case the operator shall immediately cease commercial processing and implement an emergency freeze on the disputed data pending expedited administrative adjudication to be completed within fourteen (14) days, after which confirmed resident-protected data must be purged;

(c) Implement the Inpainting Solution to remove or replace the resident's likeness from any generated, synthetic, or derivative content within seventy-two (72) hours; and

(d) Provide the resident with a cryptographically signed certificate of purge completion, transmitted via the myColorado platform.

(3) Consent mechanisms shall be designed to minimize cognitive burden on the resident. A resident may designate a fiduciary delegate, including an automated fiduciary proxy operating under the resident's DID authority, to manage consent preferences on the resident's behalf.

(4) No entity shall condition access to essential services upon the grant of a DID Handshake for data extraction unrelated to the provision of those services.

(5) Parity of Friction and Anti-Dark Pattern Mandate. The technical effort required for a resident to revoke consent must be no greater than the effort required to grant it. This mandate prohibits all dark patterns, deceptive user interface designs, or psychological manipulations intended to delay, discourage, or complicate the revocation of consent, including but not limited to:

(a) Visual interference or obscured revocation pathways;

(b) Hidden menu hierarchies that require more than two actions to access revocation settings; or

(c) Confirm-shaming or other emotive language designed to manipulate a resident's decision to revoke consent.

15-15-103. Generative Veto — Output Similarity Screening and Authorization.

(1) The state of Colorado shall establish and maintain a Hash Sentinel system that operates as

Digital severance; disconnection right. To effectuate the protections of the Digital Soul, no covered commercial operator shall employ contractual terms, software mechanisms, or service conditions that materially prevent a resident from disconnecting a resident-owned device or account from the covered operator's commercial inference engines, advertising data pipelines, or behavioral profiling systems. If a covered commercial operator degrades, disables, or withholds non-inference-dependent device functionality in response to a resident exercising Digital Soul severance or revocation rights under this article, such conduct constitutes an unfair and deceptive

trade practice subject to the remedies of this article. Nothing in this section authorizes circumvention of any technological protection measure governed by federal law.

a real-time monitoring and notification network, enabling residents to detect and veto the unauthorized generation or replication of their biometric hash by any automated system.

(2) The Hash Sentinel system shall:

(a) Operate via a Zero-Knowledge Relay such that the querying entity receives only a binary consent-or-denial response without learning the identity of the resident;

(b) Provide real-time alerts to a resident when any entity attempts to generate, derive, or replicate the resident's biometric hash; and

(c) Enable the resident to issue an immediate, irrevocable veto that halts the generation process and triggers the purge obligations of section 15-15-102.

(3) Any entity that proceeds with the generation or replication of a resident's biometric hash after receiving a veto notification shall be subject to the penalties established under the enforcement provisions of this article, including but not limited to statutory debarment by a court of competent jurisdiction.

(4) Mutual authorization for audiovisual and sensory telemetry. (a) When an audiovisual or sensory telemetry artifact reasonably contains contemporaneous telemetry of two or more identifiable residents, any real-time bypass of an otherwise applicable security screen or air-gap control for immediate presentation of such telemetry shall require affirmative authorization by each primary resident or such resident's authorized agent, including an Automated Fiduciary Proxy, using an authentication or attestation method recognized by rule. Emergency family or kinship tether access to location or safety telemetry for a minor, missing person, or incapacitated person may be authorized by rule only upon objective emergency triggers, strict time limitation, and anti-stalking safeguards, including at minimum: (I) an objective trigger such as an active Amber Alert, verified missing person report, verified imminent risk to life or serious bodily injury, or verified incapacity; (II) time-limited access not exceeding the minimum necessary and

in no event longer than eight (8) hours absent reauthorization upon renewed objective triggers; (III) immutable, tamper-evident logging of each access, ping, view, refresh, and disclosure event; (IV) protective-order and no-contact list blocks that prevent any tether access by a person subject to a restraining order, protection order, no-contact order, or analogous court order protecting the resident, and that require the system to default-deny where a match is detected; (V) notice to the resident as soon as practicable and safe, including after-the-fact notice where real-time notice would increase risk; and (VI) an always-on resident veto, override, or block capability where practicable, including a default-deny setting for adults not under guardianship, subject only to lawful process where applicable.

(b) The mutual authorization standard in this subsection (4) constitutes an exercise of the resident's property rights under the resident's master deed and shall not be construed to create any new class of public entity or to alter criminal procedure.

(c) If any primary resident denies authorization, or no authorization is received within the applicable response window, the telemetry shall remain encrypted under the administering office's custody controls as a preserved, tamper-evident non-repudiation artifact, and may be accessed only pursuant to lawful process and the confidentiality and access requirements applicable to Digital Soul artifacts.

15-15-104. Right to Automated Systems Blindness and Analog Sanctuary.

(1) Every resident of the state of Colorado shall have the right to remain invisible to automated systems. No entity operating within the state shall compel a resident to submit to biometric scanning, behavioral profiling, or algorithmic assessment as a condition of access to public spaces, government services, or essential commercial services.

(2) The state shall designate Analog Sanctuaries in each county, which shall include at minimum:

(a) One government services facility where all state and local government services available digitally are also available through non-digital means at parity of quality and timeliness;

(b) Signage and geofencing protocols ensuring that no automated data collection occurs within the boundaries of a designated Analog Sanctuary; and

(c) Annual certification by the Colorado attorney general that each designated Analog Sanctuary meets the requirements of this section and remains free of automated data collection mechanisms.

15-15-105. Compute Parity Standard.

(1) No automated decision-making system deployed within the state of Colorado shall render a consequential decision affecting a resident unless such system demonstrates Compute Parity, defined as achieving no less than ninety percent (90%) accuracy and fairness when measured against equivalent human decision-making benchmarks.

(2) Compute Parity benchmarks shall be established and updated biennially by the Colorado attorney general in consultation with the Colorado public utilities commission, using standardized testing protocols that are published on a publicly accessible website and reproducible.

(3) Any entity deploying a system that fails to meet the Compute Parity standard shall:

(a) Disclose the deficiency to all affected residents within thirty (30) days;

(b) Provide a human review option for any decision rendered by the non-compliant system; and

(c) Achieve compliance within one hundred eighty (180) days or face the graduated sanctions established under the enforcement provisions of this article.

15-15-106. Intake Firewall.

(1) Every entity that operates an automated system capable of touching or ingesting data derived from Colorado residents shall implement an Intake Firewall at the interface level of such system.

(2) The Intake Firewall shall automatically and programmatically reject any data input for which a valid DID Handshake has not been presented and cryptographically verified prior to ingestion; except that, during any phased implementation period established by rule by the Division, a

covered entity may rely upon a functionally equivalent privacy-preserving authorization method recognized by rule.

(3) Data that bypasses or is ingested in circumvention of the Intake Firewall shall be classified as Contraband Data.

(4) For purposes of this section, "discrete data input" means one distinct data record, file, or communication associated with an identifiable Colorado resident, as determined by the administering office by rule, where each such record constitutes a separate violation regardless of how it is batched, packaged, or transmitted. Each discrete data input constituting Contraband Data shall be a separate statutory violation subject to treble damages, with a statutory minimum of ten thousand dollars ($10,000) per violation, payable entirely and directly to the resident. The aggregate statutory minimum damages per enforcement action under this subsection shall not exceed the greater of ten million dollars ($10,000,000) or three times actual damages proven; a court shall reduce aggregate statutory damages upon a showing by clear and convincing evidence that the aggregate award would be grossly disproportionate to the actual harm caused and the deterrence purpose of this section.

CONSUMER PROTECTION PATCHES

15-15-107. Misappropriation of Digital Soul — Colorado Consumer Protection Act Patch.

(1) The unauthorized extraction, replication, blending, or derivative use of any component of a resident's Digital Soul, including but not limited to pixel-level and vector-level blending of likeness, shall constitute "Misappropriation of Digital Soul" under this article and a "Deceptive Trade Practice" under section 6-1-105, Colorado Revised Statutes.

(2) This section establishes a state property and consumer protection cause of action that operates independently of and is not preempted by federal copyright law, as it regulates the misappropriation of persona rather than the reproduction of copyrightable works.

(3) Treble damages shall be available under section 6-1-113, Colorado Revised Statutes, for violations of this section. All collected treble damages are payable entirely and directly to the prevailing resident.

15-15-108. Biological Product Liability — Dopamine Ceiling.

(1) The regulation of addictive design in automated systems, including but not limited to infinite scroll, autoplay, algorithmic amplification of engagement, and variable-ratio reinforcement schedules, shall be governed under health and safety product liability standards rather than speech or expression frameworks.

(2) Every automated system deployed to Colorado residents that employs engagement-maximizing design patterns shall implement a Dopamine Ceiling, which shall include:

(a) A mandatory fifteen-minute (15-minute) Hard Reset lockout triggered when a user exceeds behavioral safety thresholds as defined by the Colorado attorney general; or

(b) A Friction Mode interface that materially reduces engagement-maximizing stimuli, including but not limited to disabling autoplay, removing algorithmic recommendations, and introducing deliberate interface friction.

(c) Resident choice; default settings. For adult users, the covered operator shall provide a clear, non-deceptive choice between Hard Reset under subsection (2)(a) and Friction Mode under subsection (2)(b), with the default set to Hard Reset unless the user affirmatively opts into Friction Mode. A resident may change this setting at any time through an accessible control.

(d) Friction Mode requirements. Where a resident opts into Friction Mode, the operator shall, at a minimum, disable infinite scroll and autoplay, suppress variable-ratio reinforcement mechanics, and provide chronological or user-selected ordering options in place of default engagement-optimized ranking.

(3) Minor controls; parent/guardian override with co-management safeguards. For a minor user, the default must be the most protective version of Friction Mode and age-appropriate interaction limits established by rule. A legal parent or court-appointed guardian may override a minor’s viewing and interaction restrictions for specific services or categories, provided that: (a) the override is recorded in the minor’s guardianship log; (b) the override is revocable at any time;

and (c) where two parents or guardians have co-management authority under section 15-15-123, no single parent may permanently disable protective controls or authorize deletion actions unilaterally, absent sole legal custody or court order.

(4) Behavioral safety thresholds shall be established by the Colorado attorney general using peer-reviewed neuroscience and behavioral health research and shall be updated no less frequently than biennially.

(5) Violations of this section shall constitute product liability for neural harm and shall be subject to treble damages under section 6-1-113, Colorado Revised Statutes. All damages collected for neural harm under this section are payable entirely and directly to the prevailing resident.

15-15-117. Phased compliance — legacy systems and new systems (2027 hardware date).

(1) Legacy systems. A covered entity operating a legacy system in service as of the effective date, including covered devices and endpoints manufactured prior to January 1, 2027, may comply through software-layer gateway or interface controls that enforce consent verification, veto lists, and audit logging, including API gateway rejection, cryptographic token validation, and post-ingestion purge procedures.

(2) New systems. Any covered device, model, inference engine, or computing cluster manufactured on or after January 1, 2027, materially upgraded, or newly deployed after the compliance date established by rule shall implement the hardware-secured or enclave-level protections required by this article.

(3) Transition schedule. The office of the digital ombudsman shall set staged compliance milestones by rule.

(4) No recall mandate. Nothing in this article shall be construed to require a universal recall of consumer hardware already in the stream of commerce.

15-15-123. Minor guardianship initialization and co-management — tax-dependent linkage; no unilateral deletion.

(1) Guardianship initialization by dependent linkage. The office may establish a default minor guardianship link for purposes of administering a minor’s digital rights under this article by using objective dependent or guardianship records maintained by the Colorado department of revenue or a successor agency, including tax-return dependent associations, provided that such linkage is subject to override by a court order and subject to reasonable identity verification safeguards.

(2) Scope of guardian authority. A legal parent or court-appointed guardian may, on behalf of a minor, exercise registration, notice, access, correction, portability, and compensation-collection functions under this article where such actions are necessary to protect the minor's interests, subject to the limitations of this section and any applicable court order.

(3) Co-management; prohibition on unilateral destructive actions. No single legal parent or guardian may unilaterally authorize or execute a destructive action affecting a minor's digital rights record, including a permanent deletion request, death-purge analog, irrevocable revocation of consent, or permanent closure of a minor escrow or sovereignty account, unless:

(a) all legal parents or guardians with rights to act for the minor provide verified dual authorization; or

(b) a court of competent jurisdiction issues an order authorizing the destructive action and specifying the scope of authority.

(4) Custody dispute safeguard; preservation freeze. If a single legal parent or guardian attempts to initiate a destructive action without dual authorization, the office shall (a) deny execution, (b) place the affected record in a temporary evidence preservation freeze for not less than thirty (30) days, (c) provide notice to other known legal parents or guardians, and (d) provide an expedited process for submission of dual authorization or a court order.

(5) Construction. This section is intended to prevent unilateral erasure of family history or critical records during custody disputes while preserving the ability of guardians to protect minors' rights. Nothing in this section limits a court's authority to allocate decision-making, order protective measures, or appoint a guardian ad litem.

15-15-124. Patient-directed health record gateway — rotating access tokens; least-privilege sharing; no persistent access.

(1) Opt-in gateway. A resident may elect to access and share the resident's medical and health information through a state-administered resident interface (including MyColorado, MyApp, or a successor application) as a convenience gateway for the resident's HIPAA access, transmission, and portability rights. Election under this subsection does not require a provider to store its electronic health records on state servers and does not limit any direct provider portal access rights.

(2) Key custody; no master key. Any resident-encrypted vault or interface used under this section shall be designed so that the resident retains primary cryptographic control over resident-held access keys. The state shall not maintain

a universal decryption key for resident medical records. Nothing in this subsection prevents a covered entity from maintaining keys necessary for its own treatment operations within its own systems.

(3) Rotating access tokens; no continuous access. Access by a covered entity, provider, or authorized recipient to a resident-held or resident-gated record under this section shall be accomplished through short-lived, purpose-limited access tokens that automatically expire and are rotated on a frequent schedule established by rule. Tokens must be scoped to the minimum necessary data categories and time window required for the authorized purpose. Absent a more specific rule or shorter limit, no access token issued under this section may have a time-to-live (TTL) exceeding fifteen (15) minutes. Any reference to a “48-hour” tokenized access concept in this act shall be construed as a maximum deadline for supervisory or judicial review of an access event or token issuance and not as permission for a 48-hour token validity period for access to medical or health records.

(4) Token safeguards. At minimum, rules shall require:

(a) a maximum token time-to-live (TTL) and mandatory refresh cadence appropriate to the sensitivity of the data;

(b) automatic revocation on suspected compromise, change of guardian authority, or resident-initiated withdrawal;

(c) cryptographic binding of tokens to an authenticated device or session where feasible; and

(d) audit logging of token issuance, refresh, access events, and revocation, available to the resident in human-readable form.

(5) Break-glass exception; after-the-fact accountability. The office may authorize a narrowly tailored emergency “break-glass” access pathway for urgent treatment or safety incidents, provided that:

(a) the access is time-limited and minimum-necessary;

(b) the event is logged, notice is provided to the resident (or legal guardian) as soon as practicable, and the resident may contest misuse; and

(c) non-emergency repeated break-glass use by an entity constitutes a violation subject to enforcement under this article and any applicable state or federal law.

(6) Construction. This section is intended to prevent persistent or ambient surveillance-style access to medical records while preserving lawful clinical access and the resident's HIPAA portability rights.

Construction — opt-in; no compulsory resident enrollment.

Nothing in this act requires any resident to enroll in digital services or activate optional verification tools. Where the act offers enhanced protections through affirmative registration, the default status is non-participation unless the resident expressly opts in. Governmental access to protected systems remains subject to the condition-of-access accountability protocols established in this framework.

SEVERABILITY AND IMPLEMENTATION

15-15-109. Condition Precedent for Corporate Protections.

If any provision of this act is held invalid by a court of competent jurisdiction, such invalidity shall not affect other provisions or applications of this act that can be given effect without the invalid provision or application. This act is intended to be severable and independently operable, and no provision of this act is conditioned upon enactment, effectiveness, or continued validity of any companion measure, including any measure establishing or governing the Automation Mitigation Enterprise or any Trust structure.

However, if any provision of this act is held invalid, unconstitutional, or preempted, and such invalidity materially weakens the enforcement mechanisms or the resident's right to direct damage payouts under this act, then, as to the covered operators and covered activity to which the invalidity applies and only to that extent, any safe harbors, liability shields, or other operator-favorable defenses created by this act are proportionally suspended until constitutional compliance is restored by judicial clarification or legislative amendment. Any good-faith compliance safe harbor or similar limitation on remedies referenced in this act shall be construed narrowly and may not be

asserted by a covered operator that (a) knowingly or recklessly ingests Contraband Data, (b) suppresses, falsifies, or fails to maintain required tamper-evident audit logs after notice, (c) misrepresents compliance artifacts, or (d) fails to timely honor a resident-directed cease-processing, emergency freeze, or purge directive; and nothing in any such safe harbor shall be construed to waive, diminish, or delay any resident remedy, injunctive relief, or statutory damages otherwise available under this act or other applicable law.

15-15-110. Effective Date and Implementation Timeline.

(1) This article shall take effect upon proclamation of the governor, or, if enacted by initiative, upon the date established by the Colorado constitution for initiated measures.

(2) The myColorado Digital Deed issuance system shall be operational within one hundred eighty (180) days of the effective date.

(3) Entities subject to the Intake Firewall and Mandatory Disconnection Protocol obligations shall have three hundred sixty-five (365) days from the effective date to achieve full compliance.

(4) Entities that demonstrate good-faith compliance efforts within the first one hundred eighty (180) days shall be eligible for safe harbor protections during the compliance period; provided that any such safe harbor shall be limited to documented good-faith steps to implement required controls and shall not apply to knowing or reckless ingestion of Contraband Data, failure to honor resident revocation, cease-processing, emergency freeze, or purge directives, suppression or falsification of audit logs, or material misrepresentation of compliance artifacts, and shall not be construed to limit injunctive relief or other remedies necessary to stop ongoing harm.

ANNEX A — ENUMERATED COMPONENTS AND RULES OF CONSTRUCTION

15-15-111. Annex A — Enumerated Components of the Digital Soul.

(1) For purposes of judicial construction, statutory interpretation, and enforcement of this article, the term “Digital Soul” shall be interpreted as a composite property interest consisting

exclusively of identifiable biological, biometric, behavioral, and inference-derived data attributable to a natural person.

(2) The Digital Soul includes, but is not limited to, the following enumerated categories of data when attributable to an identifiable natural person:

(a) Biometric identifiers, including facial geometry, retinal patterns, voice prints, gait signatures, fingerprint templates, DNA-derived hashes, and other unique biological measurements capable of identifying or reidentifying a natural person;

(b) Behavioral telemetry, including clickstream data, keystroke cadence, browsing patterns, location vectors, device interaction metrics, and other measurable behavioral patterns linked to a specific natural person;

(c) Persistent unique identifiers, including device identifiers, advertising identifiers, cryptographic public keys, decentralized identifiers, or other tokens that are materially linked to a natural person;

(d) Inference outputs and predictive profiles derived from data described in subsections (2)(a) through (2)(c) of this section, when such inferences are materially attributable to and capable of affecting the rights, opportunities, or treatment of a specific natural person;

(e) Digital likeness derivatives, including synthetic renderings, generative outputs, pixel-level blends, vector-level blends, voice simulations, or other computational reproductions capable of representing or approximating the identity of a natural person.

(3) The Digital Soul does not include:

(a) Data that has been irreversibly anonymized such that no natural person can reasonably be identified directly or indirectly;

(b) Aggregated statistical data that cannot be disaggregated to identify a natural person;

(c) Information lawfully obtained and retained pursuant to a valid warrant, subpoena, or court order, provided such use remains within the scope of such legal authorization.

(4) Nothing in this Annex shall be construed to expand the scope of this article beyond identifiable data attributable to a natural person. This Annex is declaratory and interpretive in nature and does not create new administrative agencies, funding obligations, or regulatory

authorities beyond those expressly provided in this article.

(5) In the event of ambiguity, this article shall be construed in favor of protecting the resident's property interest in their Digital Soul.

SECTION __. Voluntary registration — no fee — preservation of existing remedies.

(1) Voluntary registration. Registration of a Digital Soul under this article is voluntary. No person shall be required to register as a condition of accessing public services, employment, housing, commerce, or participation in civic life.

(2) Default status. The default legal status for all residents is non-registration. Enhanced verification and enforcement mechanisms under this article are activated only upon affirmative registration by the resident.

(3) No registration fee. Registration shall not be conditioned upon payment of any fee.

(4) Preservation of existing rights. Failure to register under this article does not waive, limit, or impair any existing civil or criminal cause of action available under Colorado law.

(5) Prospective activation. Registration activates enforcement mechanisms prospectively and does not create retroactive liability for conduct occurring prior to registration, unless independently unlawful under existing law.

SECTION __. Emergency mitigation; damages construction.

(1) Emergency mitigation construction. The general assembly finds and declares that the unauthorized ingestion, exploitation, and synthetic manipulation of a resident's Digital Soul constitutes an ongoing emergency condition. Remedies, fees, statutory damages, and enforcement mechanisms authorized by this act shall be construed as emergency mitigation measures designed to remediate and deter measurable harms.

(2) Self-healing remedies. If a court of competent jurisdiction finally determines that any particular remedy, damage calculation, or enforcement mechanism in this act is unenforceable as written, the remaining remedies and enforcement provisions remain in effect, and the administering office and courts shall apply the closest lawful remedy that effectuates the deterrence and harm-mitigation purpose of this act, to the maximum extent permitted by law.

15-15-111.5. Automatic restoration question — companion ballot submission.

(1) Companion restoration submission. If a measure described in this section is submitted to the voters pursuant to the anti-dilution ratchet, the secretary of state shall also submit, as a separate ballot question at the same general election, a companion "restoration" question that asks voters whether to restore the protections, allocations, and requirements in effect immediately prior to the material reduction.

(2) Effect of restoration approval. If the voters approve the companion restoration question, the law shall be restored to the form and effect that existed immediately prior to the material reduction, notwithstanding any portion of the material reduction that may have been approved, to the extent permitted by law.

(3) Construction. This subsection is intended to ensure voters are presented with a clear, affirmative option to maintain or restore emergency mitigation protections and to prevent dilution through confusing or piecemeal amendments.

15-15-112. Capability parity access for consequential decisions — public recourse tools.

(1) Legislative declaration. The general assembly finds that automated decision systems and advanced generative artificial intelligence can be used by powerful actors to overwhelm residents in employment, housing, credit, education, and other consequential contexts. To preserve public safety, due process, and meaningful recourse, residents must have access to functionally equivalent analytical tools when such tools are used against them.

(2) Capability parity access requirement. When a covered entity uses, deploys, or relies upon an automated decision system or emergent automation system in a consequential decision affecting a Colorado resident, the resident shall be entitled to access, at no cost for personal use related to recourse, a functionally equivalent capability tier sufficient to:

(a) Understand the basis of the decision and the key factors relied upon;

(b) Generate a response, rebuttal, or clarification request;

(c) Prepare an appeal or request human review; and

(d) Exercise any rights established under this part, including verification and injunctive relief pathways.

(3) Delivery mechanisms. A covered entity may satisfy subsection (2) by providing access directly to the resident or by providing access through the public access gateway funded under title 24, article 20. Access must be timely and reasonably usable, including through the analog bridge when requested.

(4) Construction and limits. This section does not require disclosure of trade secrets or proprietary weights. The requirement is satisfied by providing functionally equivalent capability and interfaces necessary for recourse. The attorney general may adopt rules consistent with this section to ensure effective access and to prevent sham “parity” offerings.

15-15-113. Always-on generative veto and intake firewall — mandatory refusal response — non-disablement.

(1) Legislative declaration. The general assembly finds that residents must be able to revoke any digital deed lease and prevent unauthorized likeness generation in real time. Because unconsented generation can be instant and irreversible once disseminated, the protections established in sections 15-15-103 and 15-15-106 must operate continuously and shall not be subject to discretionary deactivation by covered entities.

(2) Always-on requirement. A covered entity subject to this article shall operate the Hash Sentinel veto pathway and the Intake Firewall as always-on safety and property-protection controls. A covered entity shall not offer, implement, or maintain any "off switch," administrative override, configuration flag, or product setting that disables or materially degrades:

(a) Real-time veto signaling under section 15-15-103;

(b) Contraband Data rejection at the interface level under section 15-15-106; or

(c) The revocation and cure obligations under section 15-15-102.

(3) Mandatory refusal response for likeness inputs. When a covered entity detects that a requested generation, upload, or transformation would replicate, derive, or render a resident's biometric hash without a valid active DID Handshake (or other functionally equivalent privacy-preserving authorization method recognized by rule by the Division) or after a veto signal, the entity shall:

(a) Refuse the generation or hosting action by default;

(b) Prevent completion of the generation pipeline at the interface level; and

(c) Present a clear refusal notice to the user. A compliant notice may include: "Consent not verified or revoked. Please choose another image or obtain authorization."

(4) Post-processing and lawful filtering preserved. Nothing in this section prohibits a covered entity from applying additional post-processing filters, content safety measures, or lawful moderation practices, provided such measures do not operate as a substitute for, or a disablement of, the always-on veto and Intake Firewall requirements.

(5) Enforcement and remedies. Any violation of this section constitutes a per-input violation and an unlawful practice subject to the statutory damages, injunctive relief, debarment remedies, and other enforcement mechanisms provided in this article.

SECTION __. Safety clause.

The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

SECTION __. Construction; consistency with federal law; scope.

(1) Consistency with federal law. This act shall be construed consistent with applicable federal law. Nothing in this act is intended to preempt, conflict with, or expand liability in a manner prohibited by federal law. Nothing in this act shall be construed to impose liability on any interactive computer service as defined in 47 U.S.C. § 230(f) for third-party content as provided under 47 U.S.C. § 230(c)(1). The always-on refusal and Intake Firewall requirements of this act apply solely to a covered operator's own first-party data-processing and training activities and to the operator's own generated outputs, and are not intended to impose editorial duties with respect to third-party content hosted or transmitted by an interactive computer service.

(2) Regulation of exploitation and ingestion; not editorial control. This act regulates the unauthorized ingestion, commercial exploitation, and identity-dependent processing of a resident's Digital Soul and associated protected attributes. Nothing in this act shall be construed to require any person to remove, publish, or suppress third-party speech, or to impose editorial obligations regarding third-party content, except as necessary to enforce a resident's voluntary property assertion under this act.

(3) No extraterritorial regulation. Nothing in this act regulates conduct occurring wholly outside Colorado absent a sufficient Colorado nexus, including commercial delivery to a resident of Colorado, commercial targeting of a resident of Colorado, or ingestion or processing conducted in Colorado.

(4) Notice and good-faith compliance. The administering office shall provide a free and accessible method for residents to provide notice of registration and revocation, including analog submission. A covered entity that, in good faith, uses the administering office's published verification method and honors a registered resident's opt-in selections and revocations shall be treated as acting in good faith for purposes of civil remedies under this act.

SECTION __. Emergency declaration; public safety and emergency mitigation purpose.

(1) Emergency declaration. The general assembly finds and declares that rapid advances in automated decision systems and generative artificial intelligence have created immediate and ongoing public safety threats, including identity-based exploitation, nonconsensual synthetic sexual depiction, fraud, coercion, and reputational and economic harms that cannot be prevented through private contract alone.

(2) Emergency mitigation purpose. This act establishes a voluntary, opt-in property assertion framework and enforcement mechanisms to deter and remediate these harms. The remedies, statutory damages, and enforcement tools in this act are emergency mitigation measures intended to reduce foreseeable harms and to protect residents from immediate threats to personal safety, privacy, and economic security.

(3) Public safety construction. This act shall be construed to prioritize prevention of nonconsensual synthetic depiction and identity exploitation, protection of minors and vulnerable persons, and rapid injunctive relief to stop ongoing harm, while preserving due process and the voluntary nature of registration.

15-15-118. Universal settlement eligibility; opt-in election; minor protections.

(1) Universal eligibility. Every natural person who is a Colorado resident on the settlement record date shall be an eligible claimant for the base settlement amount, regardless of age.

(2) Opt-in required. No payment shall be issued unless the claimant affirmatively elects participation in the settlement through the state-administered election process. The election process shall remain continuously available.

(3) Minor election authority. For a minor child, settlement election shall require the consent of both legal parents or guardians who share custodial or decision-making authority, unless one parent has sole legal custody as established by court order. Where sole custody exists, the sole custodial parent may elect on behalf of the minor.

(4) Minor deposit default. Settlement amounts attributable to a minor shall be deposited into the minor's protected Child Sovereignty account and shall not be withdrawn except as expressly authorized for restricted-purpose child essentials expenditures under this article.

(5) No unilateral impairment. No single parent may unilaterally authorize extraordinary withdrawals, transfers, deletion, or impairment of a minor’s protected account without either joint parental consent or court authorization.

ANNEX B — STANDARD FORMS, NOTICES, AND TECHNICAL ARTIFACTS (NONCODIFIED)

This Annex provides noncodified standard forms and technical artifacts referenced in this Act.

The Division shall publish these materials in plain language and in accessible formats without charge, including paper versions at county Analog Sanctuaries.

Digital Deed Registration Form (Opt-In) and revocation form; default status is non-registration.

Minor Dual-Consent Settlement Election Form; single-parent custody exception and dispute resolution instructions.

Parental Controls Override Authorization (parent/guardian supervision and content interaction restrictions for minors).

HIPAA Read/Share Token Request Form and token-rotation schedule disclosure (for providers and patients).

Death-Purge Directive and Family Vault carve-out notice (records preserved for lawful family history categories).

Complaint Intake Form for suspected violations (including deepfake, identity misuse, deceptive ADS, and credit-bureau harms).

Restoration Wallet / payment rail disclosure and unrestricted restitution option notice.

ANNEX C — PHASED IMPLEMENTATION AND COMPLIANCE TIMELINE (REFERENCE)

Milestone	Operational meaning
Effective Date	Launch voluntary Digital Deed registration; publish forms; open Analog Sanctuary access.
0–180 days	Good-faith safe harbor window; initial guidance; begin enforcement education.
0–365 days	Covered entities achieve compliance with intake firewall and veto/refusal response duties; legacy feasibility accommodations apply where provided.
Ongoing	Token rotation, audit logs, and resident access mechanisms maintained; anti-dilution ratchet governs weakening changes.

ANNEX D — STANDARD FORMS AND REPORTING TEMPLATES

FORM 1: NOTICE OF DIGITAL SOUL LEASE REVOCATION AND CEASE-PROCESSING DIRECTIVE

(Pursuant to Colorado Revised Statutes § 15-15-103)

WARNING TO COVERED OPERATOR (LESSEE): Under Colorado law, the individual identified below holds exclusive intangible personal property rights over their Digital Soul,

including rights of control, exclusion, and alienation. By receiving this Notice, any prior consent, terms of service, or licensing agreement granting you access to process, cache, or shadow-tag this property is immediately REVOKED. You are legally required to execute the 72-Hour Black Screen Protocol, including an emergency cease-processing freeze, enforceable suppression controls, and initiation of purge actions with tamper-evident logging sufficient for audit. Failure to comply constitutes Digital Squatting, a Class 4 Felony, and suspends your corporate liability safe harbors within the State of Colorado. Nothing in this Notice waives or limits any other remedy available to the resident or the state.

PART I: LESSOR (RESIDENT) IDENTIFICATION

* Resident Name / Authorized Agent: _____

* Sovereignty Beacon Public Hash (if applicable): _____

* Date of Revocation: _____

PART II: LESSEE (COVERED OPERATOR) IDENTIFICATION

* Entity Name: _____

* Service/Platform Known As: _____

PART III: SCOPE OF REVOCATION (Resident must select one)

[ ] GLOBAL EVICTION: Total revocation of all processing, modeling, telemetry, and inferential rendering. All historical data must be purged from active commercial modules within 72 hours.

[ ] PARTIAL/PROSTHETIC EVICTION: Revocation of commercial extraction and third-party brokering. Operator is permitted only to process data locally as an Authorized Agent (Cognitive Prosthetic) strictly for the direct benefit of the Resident.

PART IV: ATTESTATION OF THE MASTER DEED

I, the undersigned Lessor, acting under my inherent Master Deed, do hereby revoke the lease of my Digital Soul to the aforementioned Lessee. I demand immediate physical or cryptographic severance of my digital assets from your commercial inference engines.

Signature (or Cryptographic Attestation): _____

Timestamp: _____

CONSTRUCTION AND PROPORTIONAL REMEDIES

If any provision is held invalid, courts shall apply the closest lawful remedy that preserves resident consent, auditability, and the emergency mitigation purpose. Any material weakening of resident protections triggers the anti-dilution ratchet procedures in the Act.

Intent; preservation of core purpose. It is the express intent of the People that the core purpose of this Act—the mitigation of measurable externalities arising from Emergent Automation and the protection of resident sovereignty—be preserved to the maximum extent permitted by law. Any judicial finding of invalidity should be interpreted narrowly to preserve the maximum possible functionality of the Automation Mitigation Enterprise and the resident protections and safety standards established by this Act.

Severability. If any provision of this Act or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect other provisions or applications of the Act which can be given effect without the invalid provision or application, and to this end the provisions of this Act are declared to be severable, and this Act shall be given effect to the maximum extent possible notwithstanding the non-enactment, invalidation, or unavailability of any companion measure.