A COMPARISON OF THE VERSION OF
THE WASHINGTON PRIVACY ACT CONSIDERED
BY THE WASHINGTON LEGISLATURE IN 2019 (SENATE BILL 5376)
TO THE VERISON INTRODUCED ON JANUARY 14, 2020 (SENATE BILL 6281)

AN ACT Relating to the management and oversight of personal data; ~~amending RCW 43.105.369; adding a new section to chapter 9.73 RCW;~~ adding a new chapter to Title 19 RCW~~; creating new sections~~; prescribing penalties; and providing an effective date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. Sec. 1. SHORT TITLE.This act may be known and cited as the Washington privacy act.

NEW SECTION. Sec. 2. LEGISLATIVE FINDINGS.(1) The legislature finds that~~:(a) Washingtonians cherish~~ the people of Washington regard their privacy as ~~an~~ a fundamental right and an essential element of their individual freedom. Washington's Constitution explicitly provides the right to privacy, and fundamental privacy rights have long been and continue to be integral to protecting Washingtonians and to safeguarding our democratic republic.

~~(b) Washington is a technology leader on a national and global level and recognizes its distinctive position in promoting the efficient balance of consumer privacy and economic benefits.~~

~~(c) Washington explicitly recognizes its citizens' right to privacy under Article I, section 7 of the state Constitution.~~

~~(d) There is rapid~~ (2) Ongoing advances in technology have produced an exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed~~. This growth has the potential for great benefits to human knowledge, technological innovation, and economic growth, but also the potential to harm individual privacy~~ , which presents both promise and potential peril. The ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society; however, it has also created risks to privacy and freedom. The unregulated and unauthorized use and disclosure of personal information and loss of privacy can have devastating impacts, ranging from financial fraud, identity theft, and unnecessary costs, to personal time and finances, to destruction of property, harassment, reputational damage, emotional distress, and physical harm.

(3) Given that technological innovation and new uses of data can help solve societal problems and improve quality of life, the legislature seeks to shape responsible public policies where innovation and protection of individual privacy coexist. The legislature notes that our federal authorities have not developed or adopted into law regulatory or legislative solutions that give consumers control over their privacy. In contrast, the European Union's general data privacy regulation has continued to influence data privacy policies and practices of those businesses competing in global markets. In the absence of federal standards, Washington and other states across the United States are analyzing elements of the European Union's general data privacy regulation to enact state-based data privacy regulatory protections.

~~(e) Millions of Washingtonians have been affected by electronic data breaches and the resulting loss of privacy, and the net effect, both financially and in the chilling of consumer confidence, has and will continue to cost Washington state businesses.~~

~~(f) As technology and businesses continue to push the limits of data collection with exponential rapidity, laws must keep pace as technology and business practices evolve to protect businesses and consumers.~~

~~(g) There is a need to preserve individuals' trust and confidence that personal data will be protected appropriately, while supporting flexibility and the free flow of information. Meeting this need will promote continued innovation and economic growth in the networked economy.~~

(4) With this act, Washington state will be among the first tier of states giving consumers the ability to protect their own rights to privacy and requiring companies to be responsible custodians of data as technological innovations emerge. This act does so by explicitly providing consumers the right to access, correction, and deletion of personal data, as well as the right to opt out of the collection and use of personal data for certain purposes. These rights will add to, and not subtract from, the consumer protection rights that consumers already have under Washington state law.

(5) Additionally, this act imposes affirmative obligations upon companies to safeguard personal data and provide clear, understandable, and transparent information to consumers about how their personal data are used. It strengthens compliance and accountability by requiring data protection assessments in the collection and use of personal data. Finally, it empowers the state attorney general to obtain and evaluate a company's data protection assessments, to impose penalties where violations occur, and to prevent against future violations.

~~(h) Enforcement of general principles in law will ensure that citizens continue to enjoy meaningful privacy protections while affording ample flexibility for technologies and business models to evolve.~~

~~(i) The European Union recently updated its privacy law through the passage and implementation of the general data protection regulation, affording its residents the strongest privacy protections in the world. Washington residents deserve to enjoy the same level of robust privacy safeguards.~~

~~(j) In addition, the technology industry has been a tremendous driver of economic growth in Washington state. We need to ensure that any new privacy laws not only provide Washington residents with strong privacy protections but also enable industry and others to use data to create innovative technologies, products, and solutions.~~

~~(k) Technology will continue to evolve and change. Consequently, any new privacy laws must be technology neutral and flexible, so that they may apply not only to the technologies and products of today, but to the technologies and products of tomorrow.~~

~~(l) Washington residents have long enjoyed an expectation of privacy in their public movements. The development of new technology like facial recognition could, if deployed indiscriminately~~

~~and without guardrails, enable the constant surveillance of any individual any time of the day and every day of the year. Washington residents should have the right to a reasonable expectation of privacy in their movements, and thus should be free from ubiquitous and surreptitious surveillance using facial recognition technology. Further, Washington residents should have the right to expect information about the capabilities and limitations of facial recognition technology and that it should not be deployed by private sector organizations without proper public notice.~~

~~(2) As such, the legislature recognizes the consumer protection principles in this act regarding transparency, individual control, respect for context, focused collection and responsible use, security, access, and accuracy.~~

NEW SECTION. Sec. 3. DEFINITIONS.The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Affiliate" means a legal entity that shares common branding with another legal entity and that controls, is controlled by, or is under common control with, ~~another~~ that other legal entity. For these purposes, "control" or "controlled" means ownership of, or the power to vote, more than fifty percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights in section 6 (1) through (5) of this act is being made by the consumer who is entitled to exercise such rights.

~~(2~~(3) "Business associate" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

~~(3) "Business purpose" means the processing of personal data for the controller's or its processor's operational purposes, or other notified purposes, provided that the processing of personal data must be reasonably necessary and proportionate to achieve the operational purposes for which the personal data was collected or processed or for another operational purpose that is compatible with the context in which the personal data was collected. Business purposes include:~~

~~(a) Auditing related to a current interaction with the consumer and concurrent transactions including, but not limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;~~

~~(b) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;~~

~~(c) Identifying and repairing errors that impair existing or intended functionality;~~

~~(d) Short-term, transient use, provided the personal data is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction including, but not limited to, the contextual customization of ads shown as part of the same interaction;~~

~~(e) Maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;~~

~~(f) Undertaking internal research for technological development; or~~

~~(g) Authenticating a consumer's identity.~~

(4) "Child" means any natural person under thirteen years of age.

(5) "Consent" means a clear affirmative act signifying a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement~~-~~, including by electronic means, or other clear affirmative action.

(6) "Consumer" means a natural person who is a Washington resident acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

(7) "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

(8) "Covered entity" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

~~(9)(a) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.~~

~~(b) Providing publicly available information through real-time or near real-time alert services for health or safety purposes, and the collection and sale or licensing of brokered personal information incidental to conducting those activities, does not qualify the business as a data broker.~~

~~(c) The phrase "sells or licenses" does not include:~~

~~(i) A one-time or occasional sale of assets that is not part of the ordinary conduct of the business;~~

~~(ii) A sale or license of data that is merely incidental to the business; or~~

~~(iii) Providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier.~~

~~(10) "Deidentified data" means:~~

~~(a) Data that cannot be linked to a known natural person without additional information kept separately; or~~

~~(b) Data (i) that has been modified to a degree that the risk of reidentification is small, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, and (iii) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable~~

~~controls to prevent reidentification may include legal, administrative, technical, or contractual controls.~~

~~(11) "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.~~

(9) "Decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer" means decisions that include, but are not limited to, the denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water.

(10) "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such person, provided that the business that possesses the data: (a) Takes reasonable measures to ensure that the data cannot be associated with a natural person or household; (b) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and (c) contractually obligates any recipients of the information to comply with all provisions of this subsection.

(11) "Enroll," "enrolled," or "enrolling" means the process by which a facial recognition service creates a facial template from one or more images of a consumer and adds the facial template to a gallery used by the facial recognition service for identification, verification, or persistent tracking of consumers. It also includes the act of adding an existing facial template directly into a gallery used by a facial recognition service.

(12) "Facial recognition service" means technology that analyzes facial features and is used for the identification, verification, or persistent tracking of consumers in still or video images.

(13) "Facial template" means the machine-interpretable pattern of facial features that is extracted from one or more images of a consumer by a facial recognition service.

~~(12~~(14) "Health care facility" has the same meaning as in RCW 70.02.010.

~~(13~~(15) "Health care information" has the same meaning as in RCW 70.02.010.

~~(14~~(16) "Health care provider" has the same meaning as in RCW 70.02.010.

(17) "Identification" means the use of a facial recognition service by a controller to determine whether an unknown consumer matches any consumer who has been enrolled in a gallery used by the facial recognition service.

~~(15~~(18) "Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

(19) "Meaningful human review" means review or oversight by one or more individuals who are trained in accordance with section 18(9) of this act and who have the authority to alter the decision under review.

(20) "Ongoing surveillance" means tracking the physical movements of a specified individual through one or more public places over time, whether in real time or through application of a facial recognition service to historical records. It does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time after the individual has been recognized.

(21) "Persistent tracking" means the use of a facial recognition service to track the movements of a consumer on a persistent basis without recognition of that consumer. Such tracking becomes persistent as soon as:

(a) The facial template that permits the tracking uses a facial recognition service for more than forty-eight hours after the first enrolling of that template; or

(b) The data created by the facial recognition service are linked to any other data such that the consumer who has been tracked is identified or identifiable.

~~(16~~(22)(a) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data~~-~~" does not include deidentified data or publicly available information.

(b) For ~~these~~ purposes of this subsection, "publicly available information" means information that is lawfully made available from federal, state, or local government records.

~~(17~~(23) "Process" or "processing" means any operation or set of operations which are performed on personal data or on sets of personal data, whether or not by automated means, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

~~(18~~(24) "Processor" means a natural or legal person ~~that~~ who processes personal data on behalf of ~~the~~ a controller.

~~(19~~(25) "Profiling" means any form of automated processing of personal data ~~consisting of the use of personal data~~ to evaluate ~~certain personal aspects relating to a natural person~~, ~~in particular to~~ analyze~~-~~, or predict personal aspects concerning ~~that~~ an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

~~(20~~(26) "Protected health information" has the same meaning as in Title 45 C.F.R., established pursuant to the federal health insurance portability and accountability act of 1996.

~~(21) "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.~~

(27) "Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(28) "Recognition" means the use of a facial recognition service to determine whether:

(a) An unknown consumer matches any consumer who has been enrolled in a gallery used by the facial recognition service; or

(b) An unknown consumer matches a specific consumer who has been enrolled in a gallery used by the facial recognition service.

~~(22)(a)~~ (29)(a) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party ~~for purposes of licensing or selling personal data at the third party's discretion to additional third parties~~.

(b) "Sale" does not include the following: (i) The disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(30) "Security or safety purpose" means physical security, protection of consumer data, safety, fraud prevention, or asset protection.

~~(23~~(31) "Sensitive data" means (a) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, ~~or sex life or~~ sexual orientation, or citizenship or immigration status; (b) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; ~~or~~ (c) the personal data ~~of~~ from a known child; or (d) specific geolocation data. "Sensitive data" is a form of personal data.

(32) "Serious criminal offense" means any felony under chapter 9.94A RCW or an offense enumerated by Title 18 U.S.C. Sec. 2516.

(33) "Specific geolocation data" means information that directly identifies the specific location of a natural person with the precision and accuracy below one thousand seven hundred fifty feet.

~~(24)~~ (34) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained ~~or inferred over time~~ from a consumer's activities over time and across nonaffiliated web sites~~,~~ or online applications~~, or online services~~ to predict ~~user~~ such consumer's preferences or interests. It does not include advertising ~~to a consumer based upon the consumer's visits to a web site, application, or online service that a reasonable consumer would believe to be associated with the publisher where the ad is placed based on common branding, trademarks, or other indicia of common ownership, or~~ : (a) Based on activities within a controller's own web sites or online applications; (b) based on the context of a consumer's current search query or visit to a web site or online application; or (c) to a consumer in response to the consumer's request for information or feedback.

(~~25~~35) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor of the controller.

~~(26) "Verified request" means the process through which a consumer may submit a request to exercise a right or rights set forth in this chapter, and by which a controller can reasonably authenticate the request and the consumer making the request using commercially reasonable means.~~

(36) "Verification" means the use of a facial recognition service by a controller to determine whether a consumer is a specific consumer enrolled in a gallery used by the facial recognition service.

NEW SECTION. Sec. 4. JURISDICTIONAL SCOPE.(1) This chapter applies to legal entities that conduct business in Washington or produce products or services that are ~~intentionally~~ targeted to residents of Washington, and that satisfy one or more of the following thresholds:

(a) Controls or processes personal data of one hundred thousand consumers or more; or

(b) Derives over fifty percent of gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand consumers or more.

(2) This chapter does not apply to:

(a) State and local governments;

(b) Municipal corporations;

(c) Information that meets the definition of:

(i) Protected health information for purposes of the federal health insurance portability and accountability act of 1996 and related regulations;

(ii) Health care information for purposes of chapter 70.02 RCW;

(iii) Patient identifying information for purposes of 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. ~~290 dd-2~~290dd-2;

(iv) Identifiable private information for purposes of the federal policy for the protection of human subjects, 45 C.F.R. Part 46, or identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonisation, or the protection of human subjects under 21 C.F.R. Parts 50 and 56;

(v) Information and documents created specifically for, and collected and maintained by:

(A) A quality improvement committee for purposes of RCW 43.70.510, 70.230.080, or 70.41.200;

(B) A peer review committee for purposes of RCW 4.24.250;

(C) A quality assurance committee for purposes of RCW 74.42.640 or 18.20.390;

(D) A hospital, as defined in RCW 43.70.056, for reporting of health care-associated infections for purposes of RCW 43.70.056, a notification of an incident for purposes of RCW 70.56.040(5), or reports regarding adverse events for purposes of RCW 70.56.020(2)(b);

(vi) Information and documents created for purposes of the federal health care quality improvement act of 1986, and related regulations; or

(vii) Patient safety work product ~~information~~ for purposes of 42 C.F.R. Part 3, established pursuant to 42 U.S.C. Sec. 299b-21~~-26~~ through 299b-26;

(d) Information ~~maintained in the same manner as~~ originating from, and intermingled to be indistinguishable with, information under (c) of this subsection that is maintained by:

(i) A covered entity or business associate as defined by the health insurance portability and accountability act of 1996 and related regulations;

(ii) A health care facility or health care provider as defined in RCW 70.02.010; or

(iii) A program or a qualified service organization as defined by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. ~~290 dd-2~~290dd-2;

~~(e) Personal data provided to, from, or held by a consumer reporting agency as defined by 15 U.S.C. Sec. 1681a(f), and use of that data is in compliance with the federal fair credit reporting act (15 U.S.C. Sec. 1681 et seq.);~~

(e) An activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in Title 15 U.S.C. Sec. 1681a(f), by a furnisher of information, as set forth in Title 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in Title 15 U.S.C. Sec. 1861a(d), and by a user of a consumer report, as set forth in Title 15 U.S.C. Sec. 1681b.

Such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the fair credit reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the information may not be used, communicated, disclosed, or sold except as authorized by the fair credit reporting act;

(f) Personal data collected and maintained for purposes of chapter 43.71 RCW;

~~(f~~(g) Personal data collected, processed, sold, or disclosed pursuant to the federal Gramm~~-Leach~~-Leach-Bliley act (P.L. 106-102), and implementing regulations, if the collection, processing, sale, or disclosure is in compliance with that law;

~~(g~~(h) Personal data collected, processed, sold, or disclosed pursuant to the federal driver's privacy protection act of 1994 (18 U.S.C. Sec. 2721 et seq.), if the collection, processing, sale, or disclosure is in compliance with that law;~~or~~

(i) Controllers that are in compliance with the verifiable parental consent mechanisms under the children's online privacy protection act, Title 15 U.S.C. Sec. 6501 through 6506 and its implementing regulations. Controllers shall be deemed compliant with any obligation to obtain parental consent under this chapter;

(j) Personal data regulated by the federal family educations rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing regulations;

(k) Personal data regulated by the student user privacy in education rights act, chapter 28A.604 RCW; or

(~~h~~l) Data maintained for employment records purposes.

NEW SECTION. Sec. 5. RESPONSIBILITY ACCORDING TO ROLE.(1) Controllers and processors are responsible for meeting ~~the~~ their respective obligations established under this chapter.

(2) Processors are responsible under this ~~act~~ chapter for adhering to the instructions of the controller and assisting the controller to meet its obligations under this chapter. Such assistance shall include the following:

(a) Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6 of this act; and

(b) Taking into account the nature of processing and the information available to the processor, the processor shall assist the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to RCW 19.255.010; and shall provide information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 9 of this act.

(3) Notwithstanding the instructions of the controller, a processor shall:

(a) Implement and maintain reasonable security procedures and practices to protect personal data, taking into account the context in which the personal data are to be processed;

(b) Ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and

(c) Engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with subsection (5) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(~~3~~(4) Processing by a processor ~~is~~ shall be governed by a contract between the controller and the processor that is binding on ~~the processor~~ both parties and that sets out the processing instructions to which the processor is bound, including the nature and purpose of the processing, the type of personal data subject to the processing, the duration of the processing, and the

obligations and rights of both parties. In addition, the contract shall include the requirements imposed by this subsection and subsection (3) of this section, as well as the following requirements:

(a) At the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(b)(i) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this chapter; and (ii) the processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor; alternatively, the processor shall arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and audit procedure for such audits as applicable, and shall provide a report of such audit to the controller upon request.

(5) In no event shall any contract relieve a controller or a processor from the liabilities imposed on them by virtue of its role in the processing relationship as defined by this chapter.

(6) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in its processing of personal data pursuant to a controller's instructions, or that fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to such processing.

NEW SECTION. Sec. 6. CONSUMER PERSONAL DATA RIGHTS.Consumers may exercise the rights set forth in this section by submitting a request, at any time, to a controller specifying which rights the consumer wishes to exercise. In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise the rights of this chapter on the child's behalf. Except as provided in this chapter, the controller must comply with a request to exercise the rights pursuant to subsections (1) through (5) of this section.

(1) Right of access. A consumer has the right to confirm whether or not a controller is processing personal data concerning the consumer and access such personal data.

~~NEW SECTION. Sec. 6. CONSUMER RIGHTS.Controllers shall facilitate verified requests to exercise the consumer rights set forth in subsections (1) through (6) of this section.~~

~~(1) Upon a verified request from a consumer, a controller must confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data that the controller maintains in identifiable form concerning the consumer.~~

~~(a) Upon a verified request from a consumer, a controller must provide a copy of the personal data that the controller maintains in identifiable form undergoing processing. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information must be provided in a commonly used electronic form.~~

~~(b) This subsection does not adversely affect the rights or freedoms of others.~~

(2) ~~Upon a verified request from a~~ Right to correction. A consumer~~, the controller, without undue delay, must~~ has the right to correct inaccurate personal data ~~that the controller maintains in identifiable form~~ concerning the consumer~~. Taking~~ , taking into account the ~~business~~ nature of the personal data and the purposes of the processing~~, the controller must complete incomplete~~ of the personal data~~, including by means of providing a supplementary statement where appropriate~~.

~~(3)(a) Upon a verified request from a consumer, a controller must delete, without undue delay, the consumer's personal data that the controller maintains in identifiable form if one of the following grounds applies:~~

~~(i) The personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer;~~

~~(ii) For processing that requires consent under section 8(3) of this act, the consumer withdraws consent to processing and there are no business purposes for the processing;~~

~~(iii) The consumer objects to the processing pursuant to subsection (6) of this section and (A) there are no business purposes for processing the personal data for the controller, the consumer whose personal data is being processed, or the public, for which the processing is necessary; or (B) the processing is for targeted advertising;~~

~~(iv) The personal data has been unlawfully processed; or~~

~~(v) The personal data must be deleted to comply with a legal obligation under federal, state, or local law to which the controller is subject.~~

~~(b) Where the controller is obliged to delete personal data that the controller maintains in identifiable form under this section that has been disclosed to third parties by the controller, including data brokers that received the personal data through a sale, the controller must take reasonable steps, which may include technical measures, to inform other controllers of which it is aware that are processing such personal data, and that received such personal data from the controller or are processing such personal data on behalf of the controller, that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation must take into account available technology and cost of implementation.~~

~~(c) This subsection does not apply to the extent processing is necessary:~~

~~(i) For exercising the right of free speech;~~

~~(ii) For compliance with a legal obligation that requires processing of personal data by federal, state, or local law, or regulation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;~~

~~(iii) For reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;~~

~~(iv) For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing;~~

~~(v) For the establishment, exercise, or defense of legal claims;~~

~~(vi) To detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or identify, investigate, or prosecute those responsible for that activity; or~~

~~(vii) For a data broker that received the personal data from third parties and is acting as a controller, solely to prevent the personal data from reappearing in the future, in which case the controller shall instead comply with the requirements in subsection (4) of this section.~~

~~(4)(a) Upon a verified request from a consumer, the controller must restrict processing of personal data that the controller maintains in identifiable form if the purpose for which the personal data is (i) not consistent with a purpose for which the personal data was collected; (ii) not consistent with a purpose disclosed to the consumer at the time of collection or authorization; or (iii) unlawful.~~

~~(b) Where personal data is subject to a restriction of processing under this subsection, the personal data must, with the exception of storage, only be processed (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; (iii) for the protection of the rights of another natural or legal person; (iv) for reasons of important public interest under federal, state, or local law; (v) to provide products or services requested by the consumer; or (vi) for another purpose set forth in subsection (3)(c) of this section.~~

~~(c) A consumer who has obtained restriction of processing pursuant to this subsection must be informed by the controller before the restriction of processing is lifted.~~

~~(5)(a) Upon a verified request from a consumer, the controller must provide to the consumer, if technically feasible and commercially reasonable, any personal data that the controller maintains in identifiable form concerning the consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i)(A) the processing of such personal data requires consent under section 8(3) of this act, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.~~

~~(b) Requests for personal data under this subsection must be without prejudice to the other rights granted in this chapter.~~

~~(c) The rights provided in this subsection do not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and must not adversely affect the rights of others.~~

~~(6)(a) A consumer may object through a verified request, on grounds relating to the consumer's particular situation, at any time to processing of~~ (3) Right to deletion. A consumer has the right to delete personal data concerning ~~such consumer.~~ the consumer.

(4) Right to data portability. When exercising the right to access personal data pursuant to subsection (1) of this section, a consumer has the right to obtain personal data concerning the consumer, which the consumer previously provided to the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

(5) Right to opt out. A consumer has the right to opt out of the processing of personal data concerning such consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

~~(b) When a consumer objects to the processing of their personal data for targeted advertising, which includes the sale of personal data concerning the consumer to third parties for purposes of targeted advertising, the controller must no longer process the personal data subject to the objection for such purpose and must take reasonable steps to communicate the consumer's objection, unless it proves impossible or involves disproportionate effort, regarding any further processing of the consumer's personal data for such purposes to any third parties to whom the controller sold the consumer's personal data for such purposes. Third parties must honor objection requests pursuant to this subsection received from third-party controllers.~~

~~(c) If a consumer objects to processing for any purposes, other than targeted advertising, the controller may continue processing the personal data subject to the objection if the controller can demonstrate a legitimate ground to process such personal data that overrides the potential risks to the rights of the consumer associated with the processing, or if another exemption in this chapter applies.~~

~~(7) A controller must communicate any correction, deletion, or restriction of processing carried out in accordance with subsections~~ (6) Notifying third parties of consumer requests. A controller must, upon request, take reasonable steps to communicate a consumer's request to correct, delete, or opt out of the processing of personal data under subsection (2), (3), or (~~4~~5) of this section to each third ~~party recipient~~ party to whom the controller ~~knows~~ disclosed the personal data ~~has been disclosed, including third parties that received the data through a sale,~~ within one year preceding the ~~verified~~ consumer's request~~,~~ unless this proves functionally impractical, technically infeasible, or involves disproportionate effort~~, or the controller knows or is informed by the third party that the third party is not continuing to use the personal data~~. ~~The controller~~

~~must inform the consumer about third-party recipients or categories with whom the controller shares personal information, if any, if the consumer requests such information.~~

~~(8) A~~ (7) Responding to consumer requests. (a) A controller must ~~provide information on~~ inform a consumer of any action taken on a ~~verified~~ request under subsections (1) through (~~6~~5) of this section without undue delay and in any event within ~~thirty~~ forty-five days of receipt of the request. That period may be extended ~~by sixty~~ once by forty-five additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within ~~thirty~~ forty-five days of receipt of the request, together with the reasons for the delay. ~~Where the consumer makes the request by electronic means, the information must be provided by electronic means where possible, unless otherwise requested by the consumer.~~

(~~a~~(b) If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and ~~any possibility for internal review of~~ instructions for how to appeal the decision ~~by~~ with the controller as described in subsection (8) of this section.

(~~b~~c) Information provided under this section must be provided by the controller free of charge~~.~~, up to twice annually to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) Charge a reasonable fee ~~taking into account~~ to cover the administrative costs of ~~providing the information or communication or taking the action requested;~~ complying with the request, or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

~~(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request~~ (d) A controller is not required to comply with a request to exercise any of the rights under subsections (1) through (~~6~~4) of this section if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request the provision of additional information reasonably necessary to ~~confirm the identity of the consumer~~authenticate the request.

~~NEW SECTION. Sec. 7. TRANSPARENCY.(1) Controllers must be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear,~~ (8)(a) Controllers must establish an internal process whereby consumers may appeal a refusal to take action on a request to exercise any of the rights under subsections (1) through (5) of this section within a reasonable period of time after the consumer's receipt of the notice sent by the controller under subsection (7)(b) of this section.

(b) The appeal process must be conspicuously available and as easy to use as the process for submitting such requests under this section.

(c) Within thirty days of receipt of an appeal, a controller must inform the consumer of any action taken or not taken in response to the appeal, along with a written explanation of the reasons in support thereof. That period may be extended by sixty additional days where

reasonably necessary, taking into account the complexity and number of the requests serving as the basis for the appeal. The controller must inform the consumer of any such extension within thirty days of receipt of the appeal, together with the reasons for the delay. The controller must also provide the consumer with an email address or other online mechanism through which the consumer may submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general.

(d) When informing a consumer of any action taken or not taken in response to an appeal pursuant to (c) of this subsection, the controller must clearly and prominently ask the consumer whether the consumer consents to having the controller submit the appeal, along with any action taken or not taken by the controller in response to the appeal and the controller's written explanation of the reasons in support thereof, to the attorney general. If the consumer provides such consent, the controller must submit such information to the attorney general.

(e) The attorney general must make publicly available on its web site all information it receives from a controller pursuant to (d) of this subsection, except that any information that may identify a consumer shall be redacted from such information before it is made publicly available on the attorney general's web site.

NEW SECTION. Sec. 7. PROCESSING DEIDENTIFIED DATA OR PSEUDONYMOUS DATA.(1) This chapter does not require a controller or processor to do any of the following solely for purposes of complying with this chapter:

(a) Reidentify deidentified data;

(b) Comply with an authenticated consumer request to access, correct, delete, or port personal data pursuant to section 6 (1) through (4) of this act, if all of the following are true:

(i)(A) The controller is not reasonably capable of associating the request with the personal data, or (B) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

(iii) The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section; or

(c) Maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(2) The rights contained in section 6 (1) through (4) of this act do not apply to pseudonymous data in cases where the controller is able to demonstrate that it is not in a position to identify the consumer, for instance, due to the institution of effective technical and organizational controls

that prevent the controller from accessing information that would enable the identification of the consumer.

(3) A controller that uses pseudonymous data or deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or deidentified data are subject, and must take appropriate steps to address any breaches of contractual commitments.

NEW SECTION. Sec. 8. RESPONSIBILITIES OF CONTROLLERS.(1) Transparency.

(a) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(i) The categories of personal data processed by the controller;

~~(a) The~~ (ii) The purposes for which the categories of personal data ~~collected by the controller~~are processed;

(iii) How and where consumers may exercise the rights contained in section 6 of this act, including how a consumer may appeal a controller's action with regard to the consumer's request;

~~(b~~(iv) The ~~purposes for which the~~ categories of personal data ~~is used and disclosed to~~ that the controller shares with third parties, if any; and

~~(c) The rights that consumers may exercise pursuant to section 6 of this act, if any;~~

~~(d) The categories of personal data that the controller shares with third parties, if any; and~~

~~(e~~(v) The categories of third parties, if any, with whom the controller shares personal data.

(~~2~~b) If a controller sells personal data to ~~data brokers~~ third parties or processes personal data for targeted advertising, it must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to ~~object to~~ opt out of such processing, in a clear and conspicuous manner.

(c) Controllers shall not require a consumer to create a new account in order to exercise a right, but a controller may require a consumer to use an existing account to exercise the consumer's rights under this chapter.

(2) Purpose specification. A controller's collection of personal data must be limited to what is reasonably necessary in relation to the specified and express purposes for which such data are processed, as disclosed to the consumer.

(3) Data minimization. A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified and express purposes for which such data are processed, as disclosed to the consumer.

(4) Avoid secondary use. Except as provided in this chapter, a controller may not process personal data for purposes that are not reasonably necessary to, or compatible with, the specified

and express purposes for which such personal data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(5) Security. A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue.

(6) Nondiscrimination. A controller may not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer.

(7) Sensitive data. A controller may not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of personal data concerning a known child, without obtaining consent from the child's parent or lawful guardian.

(8) Nonwaiver of consumer rights. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter shall be deemed contrary to public policy and shall be void and unenforceable.

NEW SECTION. Sec. ~~8~~9. ~~RISK~~ DATA PROTECTION ASSESSMENTS.(1) Controllers must conduct, to the extent not previously conducted, a ~~risk~~ data protection assessment of each of their processing activities involving personal data and an additional ~~risk~~ data protection assessment any time there is a change in processing that materially increases the risk to consumers. Such ~~risk~~ data protection assessments must take into account the type of personal data to be processed by the controller, including the extent to which the personal data ~~is~~ are sensitive data or otherwise sensitive in nature, and the context in which the personal data ~~is~~ are to be processed.

(2) ~~Risk~~ Data protection assessments conducted under subsection (1) of this section must identify and weigh the benefits that may flow directly and indirectly from the processing to the controller, consumer, other stakeholders, and the public~~,~~ against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, must ~~factor~~ be factored into this assessment by the controller.

(3) If the ~~risk~~ data protection assessment conducted under subsection (1) of this section determines that the potential risks of privacy harm to consumers are substantial and outweigh the interests of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer or if another exemption under this chapter applies. To the extent the controller seeks consumer consent for processing, such consent ~~shall~~ must be as easy to withdraw as to give.

(4) Processing ~~for a business purpose~~ shall be presumed to be permissible unless: (a) It involves the processing of sensitive data; and (b) the risk of processing cannot be reduced ~~through the use of~~ by appropriate administrative and technical safeguards.

(5) The attorney general may request, in writing, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. The controller must make ~~the risk~~ a data protection assessment available to the attorney general upon ~~request. Risk~~ such a request. The attorney general may evaluate the data protection assessments for compliance with the duties contained in section 8 of this act and with other laws including, but not limited to, chapter 19.86 RCW. Data protection assessments are confidential and exempt from public inspection and copying under chapter 42.56 RCW. The disclosure of a data protection assessment pursuant to a request from the attorney general under this subsection does not constitute a waiver of the attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

~~NEW SECTION. Sec. 9. DEIDENTIFIED DATA.A controller or processor that uses deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the deidentified data is subject, and must take appropriate steps to address any breaches of contractual commitments.~~

NEW SECTION. Sec. 10. ~~EXEMPTIONS.(1~~LIMITATIONS AND APPLICABILITY.(1) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to:

(a) Comply with federal, state, or local laws, rules, or regulations;

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local ~~law~~laws, rules, or regulations;

(d) Investigate, establish, exercise, prepare for, or defend legal claims;

~~(e) Prevent or detect identity theft, fraud, or other criminal activity or verify identities;~~

~~(f) Perform~~ (e) Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party ~~or in order to~~ , or take steps at the request of the consumer prior to entering into a contract;

(~~g~~f) Protect the vital interests of the consumer or of another natural person;

~~(h) Perform a task carried out in the public interest or in the exercise of official authority vested in the controller;~~

~~(i) Process personal data of a consumer for one or more specific purposes where the consumer has given their consent to the processing; or~~

~~(j)~~(g) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action~~.~~;

(h) Process personal data for reasons of public interest in the areas of public health, or generalizable scientific, historical, or statistical research, but solely to the extent that the processing is (i) subject to suitable and specific measures to safeguard the rights of the consumer; and (ii) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law; or

(i) Assist another controller, processor, or third party with any of the obligations under this subsection.

(2) The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to collect, use, or retain data to:

(a) Conduct internal research to improve, repair, or develop products, services, or technology;

(b) Identify and repair technical errors that impair existing or intended functionality; or

(c) Perform internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the controller, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

~~(2~~(3) The obligations imposed on controllers or processors under this chapter do not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under Washington law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Washington law as part of a privileged communication.

(~~3~~4) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this chapter is not in violation of this chapter~~, including under section 11 of this act,~~ if the recipient processes such personal data in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not ~~liable under~~ in violation of this chapter~~, including under section 11 of this act,~~ for the obligations of ~~a~~ the controller or processor ~~to~~ from which it ~~provides services~~receives such personal data.

~~(4) This chapter does not require a controller or processor to do the following:~~

~~(a) Reidentify deidentified data;~~

~~(b) Retain, link, or combine personal data concerning a consumer that it would not otherwise retain, link, or combine in the ordinary course of business;~~

~~(c) Comply with a request to exercise any of the rights under section 6 (1) through (6) of this act if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.~~

(5) Obligations imposed on controllers and processors under this chapter ~~do~~ shall not:

(a) Adversely affect the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution; or

(b) Apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

(6) Personal data that are processed by a controller pursuant to this section must not be processed for any purpose other than those expressly listed in this section. Personal data that are processed by a controller pursuant to this section may be processed solely to the extent that such processing is: (i) Necessary, reasonable, and proportionate to the specific purpose or purposes listed in this section; and (ii) adequate, relevant, and limited to what is necessary in relation to the specific purpose or purposes listed in this section. Furthermore, personal data that are collected, used, or retained pursuant to subsection (2) of this section must, insofar as possible, taking into account the nature and purpose or purposes of such collection, use, or retention, be subjected to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data, and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

(7) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (6) of this section.

(8) Processing personal data solely for the purposes expressly identified in subsection (1)(a) through (d) or (g) of this section does not, by itself, make an entity a controller with respect to such processing.

NEW SECTION. Sec. 11. LIABILITY.(1) ~~This~~ Any violation of this chapter ~~does~~ shall not serve as the basis for~~-~~, or be subject to, a private right of action under this chapter or ~~any other law~~ under any other law. This does not relieve any party from any duties or obligations imposed, or to alter any independent rights that consumers have under other laws, chapter 19.86 RCW, the Washington state Constitution, or the United States Constitution.

(2) Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this chapter, the liability ~~shall~~ must be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

~~NEW SECTION. Sec. 12. ENFORCEMENT.(1) The legislature finds that the practices covered by this chapter are matters vitally affecting the public interest for the purpose of applying the consumer protection act, chapter 19.86 RCW. A violation of this chapter is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade~~

~~or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW.~~

~~(2) The~~ NEW SECTION. Sec. 12. ENFORCEMENT.(1) The attorney general ~~may bring~~ has exclusive authority to enforce this chapter by bringing an action in the name of the state, or as parens patriae on behalf of persons residing in the state~~, to enforce this chapter~~.

(~~3~~2) ~~A controller or processor is in violation of this chapter if it fails to cure any alleged violation of sections 6 through 10 of this act within thirty days after receiving notice of alleged noncompliance.~~ Any controller or processor that violates this chapter is subject to an injunction and liable for a civil penalty of not more than ~~two thousand five hundred dollars for each violation or~~ seven thousand five hundred dollars for each ~~intentional~~ violation.

~~(4)~~ NEW SECTION. Sec. 13. CONSUMER PRIVACY ACCOUNT.The consumer privacy account is created in the state treasury. All receipts from the imposition of civil penalties under this chapter must be deposited into the account except for the recovery of costs and attorneys' fees accrued by the attorney general in enforcing this chapter. Moneys in the account may be spent only after appropriation. ~~Expenditures from~~ Moneys in the account may only be used ~~only to fund~~ for the purposes of the office of privacy and data protection as ~~established~~ created under RCW 43.105.369, and may not be used to supplant general fund appropriations to the agency.

NEW SECTION. Sec. ~~13~~14. PREEMPTION.This chapter supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by controllers or processors.

NEW SECTION. Sec. ~~14~~15. ~~FACIAL RECOGNITION.(1~~PRIVACY OFFICE STUDY.(1) ~~Controllers using facial recognition for profiling must employ meaningful human review prior to making final decisions based on such profiling where such final decisions~~ The state office of privacy and data protection shall conduct a study on the development of technology, such as a browser setting, browser extension, or global device setting, indicating a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning consumers or similarly significant effects concerning consumers.~~Decisions producing legal effects or similarly significant effects shall include, but not be limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.~~

(2) The office of privacy and data protection shall submit a report of its findings and recommendations to the governor and the appropriate committees of the legislature by October 31, 2021.

NEW SECTION. Sec. 16. ATTORNEY GENERAL REPORT.(1) The attorney general shall compile a report evaluating the liability and enforcement provisions of this chapter including, but not limited to, the effectiveness of its efforts to enforce this chapter, and any recommendations for changes to such provisions.

(2) The attorney general shall submit the report to the governor and the appropriate committees of the legislature by July 1, 2022.

NEW SECTION. Sec. 17. JOINT RESEARCH INITIATIVES.The governor may enter into agreements with the governments of the Canadian province of British Columbia and the states of California and Oregon for the purpose of sharing personal data or personal information by public bodies across national and state borders to enable collaboration for joint data-driven research initiatives. Such agreements must provide reciprocal protections that the respective governments agree appropriately safeguard the data.

NEW SECTION. Sec. 18. FACIAL RECOGNITION.(1) Processors that provide facial recognition services must make available an application programming interface or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent, and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations. Such subpopulations may be defined by race, skin tone, ethnicity, gender, age, disability status, or other protected characteristic that is objectively determinable or self-identified by the individuals portrayed in the testing dataset. If the results of that independent testing identify material unfair performance differences across subpopulations and those results are disclosed directly to the processor, who, acting reasonably, determines that the methodology and results of that testing are valid, then the processor must develop and implement a plan to address the identified performance differences. Nothing in this subsection prevents a processor from prohibiting the use of the processor's facial recognition service by a competitor for competitive purposes.

(2) Processors that provide facial recognition services must provide documentation that includes general information that ~~explains~~ :

(a) Explains the capabilities and limitations of the ~~technology in terms that customers and consumers can understand.~~services in plain language; and

(b) Enables testing of the services in accordance with this section.

(3) Processors that provide facial recognition services must prohibit, in the contract required by section 5 of this act, the use of ~~such~~ facial recognition services by controllers to unlawfully discriminate under federal or state law against individual consumers or groups of consumers.

~~(4) Controllers must obtain consent from consumers prior to deploying facial recognition services in physical premises open to the public. The placement of conspicuous notice in physical premises that clearly conveys that facial recognition services are being used constitute a consumer's consent to the use of such facial recognition services when that consumer enters those premises that have such notice.~~

~~(5) Providers of commercial facial recognition services that make their technology available as an online service for developers and customers to use in their own scenarios must make available an application programming interface or other technical capability, chosen by the provider, to enable third parties that are legitimately engaged in independent testing to conduct reasonable tests of those facial recognition services for accuracy and unfair bias.~~

~~(6) For purposes of this section, "facial recognition" means technology that analyzes facial features and is used for the unique personal identification of natural persons in still or video images.~~

~~NEW SECTION. Sec. 15. A new section is added to chapter 9.73 RCW to read as follows:~~

~~(1) State and local government agencies shall not use facial recognition technology to engage in ongoing surveillance of specified individuals in public spaces, unless such use is in support of law enforcement activities and either (a) a court order has been obtained to permit the use of facial recognition services for that ongoing surveillance; or (b) where there is an emergency involving imminent danger or risk of death or serious physical injury to a person.~~

~~(2) This section applies to all Washington state and local government agencies.~~

~~(3) For purposes of this section, "facial recognition" means the same as in section 14 of this act.~~

~~Sec. 16. RCW 43.105.369 and 2016 c 195 s 2 are each amended to read as follows:~~

~~(1) The office of privacy and data protection is created within the office of the state chief information officer. The purpose of the office of privacy and data protection is to serve as a central point of contact for state agencies on policy matters involving data privacy and data protection.~~

~~(2) The director shall appoint the chief privacy officer, who is the director of the office of privacy and data protection.~~

~~(3) The primary duties of the office of privacy and data protection with respect to state agencies are:~~

~~(a) To conduct an annual privacy review;~~

~~(b) To conduct an annual privacy training for state agencies and employees;~~

~~(c) To articulate privacy principles and best practices;~~

~~(d) To coordinate data protection in cooperation with the agency; and~~

~~(e) To participate with the office of the state chief information officer in the review of major state agency projects involving personally identifiable information.~~

~~(4) The office of privacy and data protection must serve as a resource to local governments and the public on data privacy and protection concerns by:~~

~~(a) Developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting a training program or programs for local governments; and~~

~~(b) Educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect this information.~~

~~(5) By December 1, 2016, and every four years thereafter, the office of privacy and data protection must prepare and submit to the legislature a report evaluating its performance. The office of privacy and data protection must establish performance measures in its 2016 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been achieved. These performance measures must include, but are not limited to, the following:~~

~~(a) The number of state agencies and employees who have participated in the annual privacy training;~~

~~(b) A report on the extent of the office of privacy and data protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity;~~

~~(c) A report on the implementation of data protection measures by state agencies attributable in whole or in part to the office of privacy and data protection's coordination of efforts; and~~

~~(d) A report on consumer education efforts, including but not limited to the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the office of privacy and data protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.~~

~~(6) Within one year of June 9, 2016, the office of privacy and data protection must submit to the joint legislative audit and review committee for review and comment the performance measures developed under subsection (5) of this section and a data collection plan.~~

~~(7) The office of privacy and data protection shall submit a report to the legislature on the: (a) Extent to which telecommunications providers in the state are deploying advanced telecommunications capability; and (b) existence of any inequality in access to advanced telecommunications infrastructure experienced by residents of tribal lands, rural areas, and economically distressed communities. The report may be submitted at a time within the discretion of the office of privacy and data protection, at least once every four years, and only to the extent the office of privacy and data protection is able to gather and present the information within existing resources.~~

~~(8) The office of privacy and data protection must conduct an analysis on the public sector use of facial recognition. By September 30, 2023, the office of privacy and data protection must submit a report of its findings to the appropriate committees of the legislature.~~

~~(9) The office of privacy and data protection, in consultation with the attorney general, must by rule (a) establish any exceptions to this chapter necessary to comply with state or federal law by the effective date of this section and as necessary thereafter, (b) clarify definitions of this chapter as necessary, and (c) create exemption eligibility requirements for small businesses and research institutions.~~

(4) Controllers must provide a conspicuous and contextually appropriate notice whenever a facial recognition service is deployed in a physical premise open to the public that includes, at minimum, the following:

(a) The purpose or purposes for which the facial recognition service is deployed; and

(b) Information about where consumers can obtain additional information about the facial recognition service including, but not limited to, a link to any applicable online notice, terms, or policy that provides information about where and how consumers can exercise any rights that they have with respect to the facial recognition service.

(5) Controllers must obtain consent from a consumer prior to enrolling an image of that consumer in a facial recognition service used in a physical premises open to the public.

(6) Except as provided in subsection (5) of this section, controllers may enroll an image of a consumer in a facial recognition service for a security or safety purpose without first obtaining consent from that consumer, provided that all of the following requirements are met:

(a) The controller must hold a reasonable suspicion, based on a specific incident, that the consumer has engaged in criminal activity, which includes, but is not limited to, shoplifting, fraud, stalking, or domestic violence;

(b) Any database used by a facial recognition service for identification, verification, or persistent tracking of consumers for a security or safety purpose must be used solely for that purpose and maintained separately from any other databases maintained by the controller;

(c) The controller must review any such database used by the controller's facial recognition service no less than biannually to remove facial templates of consumers whom the controller no longer holds a reasonable suspicion that they have engaged in criminal activity or that are more than three years old; and

(d) The controller must establish an internal process whereby a consumer may correct or challenge the decision to enroll the image of the consumer in a facial recognition service for a security or safety purpose.

(7) Controllers using a facial recognition service to make decisions that produce legal effects on consumers or similarly significant effects on consumers must ensure that those decisions are subject to meaningful human review.

(8) Prior to deploying a facial recognition service in the context in which it will be used, controllers must test the facial recognition service in operational conditions. Controllers must take commercially reasonable steps to ensure best quality results by following all reasonable guidance provided by the developer of the facial recognition service.

(9) Controllers using a facial recognition service must conduct periodic training of all individuals that operate a facial recognition service or that process personal data obtained from the use of facial recognition services. Such training shall include, but not be limited to, coverage of:

(a) The capabilities and limitations of the facial recognition service;

(b) Procedures to interpret and act on the output of the facial recognition service; and

(c) The meaningful human review requirement for decisions that produce legal effects on consumers or similarly significant effects on consumers, to the extent applicable to the deployment context.

(10) Controllers shall not knowingly disclose personal data obtained from a facial recognition service to a law enforcement agency, except when such disclosure is:

(a) Pursuant to the consent of the consumer to whom the personal data relates;

(b) Required by federal, state, or local law in response to a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer or grand jury;

(c) Necessary to prevent or respond to an emergency involving danger of death or serious physical injury to any person, upon a good faith belief by the controller; or

(d) To the national center for missing and exploited children, in connection with a report submitted thereto under Title 18 U.S.C. Sec. 2258A.

(11) Controllers and processors that deploy a facial recognition service must respond to a consumer request to exercise the rights specified in section 6 of this act and must fulfill the duties identified in section 8 of this act.

~~NEW SECTION. Sec. 17. Sections 3 through 14~~ NEW SECTION. Sec. 19. Sections 1 through 18 and 20 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. Sec. ~~18~~20. ~~This~~ Except for section 15 of this act, this act takes effect July 31, 2021.