S-1870.3

SUBSTITUTE SENATE BILL 5377

State of Washington 66th Legislature 2019 Regular Session

By Senate Environment, Energy & Technology (originally sponsored by Senators Carlyle, Palumbo, Mullet, Hasegawa, Keiser, Pedersen, and Saldaña)

READ FIRST TIME 02/21/19.

AN ACT Relating to data sales and governance; amending RCW 43.105.020; adding new sections to chapter 43.105 RCW; creating new sections; and providing an expiration date.

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

NEW SECTION. **Sec. 1.** This act may be known and cited as the data management and protection act.

NEW SECTION. **Sec. 2.** The legislature finds that:

(1) The Constitution and laws of the state of Washington provide for robust protection of personal privacy;

(2) Data breaches and internet crime have in recent years repeatedly compromised the safety and welfare of Washington residents and visitors;

(3) The people of the state expect and require their government to act as a good steward of all data with which it is entrusted;

(4) The public entrusts the state of Washington with their data and expects that it will be treated with a high degree of professionalism;

(5) The trust of the public is more valuable to the state than any funds to be derived from selling data;

(6) The legislature has only rarely deemed the sale of data to be in the public interest;

(7) The legislature created the office of privacy and data protection in part to enhance the practice of data stewardship among state agencies and local government;

(8) The people of the state expect state agencies to appropriately protect especially vulnerable people from unwarranted exposure, danger, or interference;

(9) The state's partners including businesses, governments, and other organizations are held to no lesser account than state agencies when conducting or supporting state functions;

(10) The state strives to make decisions based only on the best data available in order to ensure fairness and efficiency in the conduct of government; and

(11) Transparency and open data have been a priority for the legislature since the creation of the information access task force in 1995.

Sec. 3. RCW 43.105.020 and 2017 c 92 s 2 are each amended to read as follows:

The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Agency" means the consolidated technology services agency.

(2) "Board" means the technology services board.

(3) "Customer agencies" means all entities that purchase or use information technology resources, telecommunications, or services from the consolidated technology services agency.

(4) "Director" means the state chief information officer, who is the director of the consolidated technology services agency.

(5) "Enterprise architecture" means an ongoing activity for translating business vision and strategy into effective enterprise change. It is a continuous activity. Enterprise architecture creates, communicates, and improves the key principles and models that describe the enterprise's future state and enable its evolution.

(6) "Equipment" means the machines, devices, and transmission facilities used in information processing, including but not limited to computers, terminals, telephones, wireless communications system facilities, cables, and any physical facility necessary for the operation of such equipment.

(7) "Information" includes, but is not limited to, data, text, voice, and video.

(8) "Information security" means the protection of communication and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to:

(a) Prevent improper information modification or destruction;

(b) Preserve authorized restrictions on information access and disclosure;

(c) Ensure timely and reliable access to and use of information; and

(d) Maintain the confidentiality, integrity, and availability of information.

(9) "Information technology" includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, radio technologies, and all related interactions between people and machines.

(10) "Information technology portfolio" or "portfolio" means a strategic management process documenting relationships between agency missions and information technology and telecommunications investments.

(11) "K-20 network" means the network established in RCW 43.41.391.

(12) "Local governments" includes all municipal and quasi-municipal corporations and political subdivisions, and all agencies of such corporations and subdivisions authorized to contract separately.

(13) "Office" means the office of the state chief information officer within the consolidated technology services agency.

(14) "Oversight" means a process of comprehensive risk analysis and management designed to ensure optimum use of information technology resources and telecommunications.

(15) "Proprietary software" means that software offered for sale or license.

(16) "Public agency" means any agency of this state or another state; any political subdivision or unit of local government of this state or another state including, but not limited to, municipal corporations, quasi-municipal corporations, special purpose

districts, and local service districts; any public benefit nonprofit corporation; any agency of the United States; and any Indian tribe recognized as such by the federal government.

(17) "Public benefit nonprofit corporation" means a public benefit nonprofit corporation as defined in RCW 24.03.005 that is receiving local, state, or federal funds either directly or through a public agency other than an Indian tribe or political subdivision of another state.

(18) "Public record" has the definitions in RCW 42.56.010 and chapter 40.14 RCW and includes legislative records and court records that are available for public inspection.

(19) "Public safety" refers to any entity or services that ensure the welfare and protection of the public.

(20) "Security incident" means an accidental or deliberative event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources.

(21) "State agency" means every state office, department, division, bureau, board, commission, or other state agency, including offices headed by a statewide elected official.

(22) "Telecommunications" includes, but is not limited to, wireless or wired systems for transport of voice, video, and data communications, network systems, requisite facilities, equipment, system controls, simulation, electronic commerce, and all related interactions between people and machines.

(23) "Utility-based infrastructure services" includes personal computer and portable device support, servers and server administration, security administration, network administration, telephony, email, and other information technology services commonly used by state agencies.

(24) "Consent" means a clear, affirmative act establishing 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 or other clear, affirmative action.

(25) "Consumer" means a natural person who is a Washington resident, property owner, or a beneficiary of the state. "Consumer" does not include an employee or contractor of a business acting in their role as an employee or contractor. "Consumer" does not include inmates under the jurisdiction of the department of corrections.

(26) "Deidentified data" means data that: (a) Cannot be linked to a known natural person without additional information kept separately; or (b)(i) has been modified to a degree that the risk of reidentification is small, or (ii) a state agency has committed to not attempt to reidentify.

(27) "Identified or identifiable natural person" means a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(28) "Personal data" means any information collected by a state agency or entity relating to an identified or identifiable natural person. "Personal data" does not include deidentified data or health care, financial, or educational data protected by federal law.

(29) "Personal information" means any information relating to an identified or identifiable natural person. "Personal data" does not include deidentified data or health care, financial, or educational data protected by federal law.

(30) "Process" or "processing" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion, or destruction.

(31) "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 aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

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

(33) "Sale" means the exchange of personal data for monetary consideration to a third party for purposes of aggregating and licensing or disclosing personal data at the third party's discretion to additional third parties. "Sale" does not include the disclosure of personal data to a third party, such as another state agency or branch of government, 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 state agency. "Sale" does not include cost recovery as permitted under RCW 42.56.120 or existing record or management practices regarding vital statistics.

(34) "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.

NEW SECTION. **Sec. 4.** A new section is added to chapter 43.105 RCW to read as follows:

(1) The sale of personal data to third parties by state agencies is prohibited except as authorized by law. For the avoidance of doubt, any such sale of personal data that fails to comply with the requirements of this chapter is impermissible.

(2) State agencies authorized by law to sell information containing the personal data of individuals to third parties must take affirmative steps, including but not limited to those set forth in this chapter, to protect such data from impermissible subsequent use, transfer, or sale by such third parties.

(3) Before completing a sale of personal data or confidential data to an entity other than the subject of such data, a state agency must confirm that the conditions under which the data is to be used are documented in a contract involving one or more state agencies providing the data.

(a) The contract must include the following requirements at a minimum:

(i) A data recipient must undergo both permissible use and data security audits prior to receiving data and on a reoccurring basis;

(ii) A data security audit must verify at a minimum compliance with the data security standards adopted by the office of the chief information officer, or equivalent;

(iii) A permissible use audit must verify at a minimum compliance with permissible use standards adopted by the state agency;

(iv) A data recipient that shares data with other entities must:

(A) Enter into a contract that includes at a minimum the data security, permissible use, and audit requirements set forth in the contract;

(B) Require the data recipient to ensure that subsequent recipients comply with the data security, permissible use, and audit requirements; and

(C) Other requirements as may be required by the office of the chief information officer; and

(v) A provision that the cost of the audits performed pursuant to this subsection must be borne by the data recipient. A new data recipient must bear the initial cost to set up a system to disburse the data to the data recipient.

(b) Data security audits required under this section must be conducted in accordance with professional audit standards by individuals with nationally recognized certifications relevant to the type of audit performed.

(c) A state agency may accept an audit meeting the requirements of this section that was conducted within the previous year.

(4)(a) State agencies may charge a fee in connection with the dissemination of personal data under this section, as authorized by law, or for the purpose of recovering processing costs.

(b) State agencies must use any moneys collected under this subsection solely for the purposes of technology improvement, data management, and data audit functions.

(5) If a list or other compilation of personal data is used for any purpose other than that authorized in this section, the agent or contractor responsible for the unauthorized disclosure or use must be denied further access to such information by the state agency.

(6) Nothing in this section shall be construed to relieve any state agency of any obligation imposed by chapter 19.255 RCW.

(7) The requirements of this section do not apply to the following:

(a) Public records disclosed pursuant to the public records act, chapter 42.56 RCW, and related law;

(b) Release of records for research pursuant to chapter 42.48 RCW;

(c) Review, release, or correction of data by the individual who is the subject of the data, pursuant to RCW 43.105.365;

(d) Voluntary publication of open data via state systems that are widely accessible by the public pursuant to RCW 43.105.365; or

(e) Campaign disclosure and contribution data published pursuant to chapter 42.17A RCW.

NEW SECTION. **Sec. 5.** A new section is added to chapter 43.105 RCW to read as follows:

The office of privacy and data protection must publish among its privacy principles and best practices the following statement of principles to promote responsible stewardship of the state's structured data assets:

(1) Data minimization: Data access, collection, and processing should be kept to the minimum amount necessary to fulfill its purpose.

(a) The retention of data should have a legitimate and fair basis, including beyond the purposes for which access to the data was originally granted, to ensure that no extra or just-in-case data set is stored.

(b) Any data retention should be also considered in light of the potential risks, harms, and benefits. The data should be permanently deleted upon conclusion of the time period needed to fulfill its purpose.

(2) Due diligence: Third-party collaborators engaging in data use should act in compliance with relevant laws, including privacy laws, as well as the highest standards of confidentiality.

(a) Third-party collaborators' actions should adhere to the same principles as public agencies.

(b) Legally binding agreements outlining parameters for data access and handling, including but not limited to data security, data formats, data transmission, fusion, analysis, validation, storage, retention, reuse, licensing, and disposition, should be established to ensure reliable and secure access to data provided by third-party collaborators.

(3) Sensitive data and sensitive contexts: Stricter standards of data protection should be employed while obtaining, accessing, collecting, analyzing, or otherwise using data on vulnerable populations and persons at risk, children and young people, or any other sensitive data.

(4) Data quality: Data and information are critical to effective business decision making in government and should be maintained in a manner appropriate to meet business needs.

(a) Data and information that is used by multiple applications or shared across business units should be defined and managed from an enterprise perspective and fit for a variety of purposes.

(b) All data-related activities should be designed, carried out, reported, and documented accurately. More specifically, data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity, and coherence, and be kept up to date.

(c) Data quality should be carefully considered in light of the risks that the use of low-quality data for decision making can create for individuals and groups.

(5) Open data, transparency and accountability: Transparency is a critical element of accountability. Being transparent about data use, including but not limited to publishing data sets or publishing an organization's data use practices, is generally encouraged, but should be balanced against privacy, justice, and environmental stewardship.

(a) Except in cases where there is a legitimate reason not to do so, the existence, description, meaning, authorship, location, age, and purpose of data use should be publicly disclosed and described in a clear and nontechnical language suitable for a general audience.

(b) Open data is an important driver of innovation, transparency, and accountability. Therefore, whenever possible, the data should be made open unless there are legitimate reasons not to do so.

(6) Data security: Data security is crucial in ensuring data privacy and data protection. Taking into account available technology and cost of implementation, robust technical and organizational safeguards and procedures, including efficient monitoring of data access and data breach notification procedures, should be implemented to ensure proper data management throughout the data life cycle and prevent any unauthorized use, disclosure, or breach of personal data.

(a) No deidentified data should knowingly and purposely be reidentified, unless there is a legitimate, lawful, and fair basis for doing so.

(b) Data access should be limited to authorized personnel, based on the "need-to-know" principle.

(c) Personnel should undergo regular and systematic data privacy and data security trainings.

(d) Prior to data use, vulnerabilities of the security system, including but not limited to data storage and way of transfer, should be assessed.

NEW SECTION. **Sec. 6.** A new section is added to chapter 43.105 RCW to read as follows:

By June 1, 2020, the chief privacy officer shall present to the relevant committees of the legislature a report proposing how state agencies should treat personal data and respond to verified requests for personal data from consumers. In the creating the report, the chief privacy officer shall:

(1) Collaborate with state agencies;

(2) Include proposed legislation;

(3) Detail methods for state agencies to comply with the proposed legislation; and

(4) Consider whether:

(a) Agencies should receive exemptions because complying with the proposed legislation would impose a substantial financial burden.

(b) Agencies should provide access to personal data that the agency maintains in identifiable form concerning the consumer.

(c) Agencies should provide a copy of the personal data that the agency maintains in identifiable form when undergoing processing.

(d) Agencies should correct inaccurate personal data that the agency maintains in identifiable form concerning the consumer.

(e) Agencies should delete the consumer's personal data that the agency maintains in identifiable form without undue delay where the personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed, subject to chapter 42.56 RCW.

(f) Agencies should restrict processing of personal data that the agency maintains in identifiable form if one of the following grounds applies:

(i) The accuracy of the personal data is contested by the consumer, for a period enabling the agency to verify the accuracy of the personal data;

(ii) The processing is unlawful and the consumer opposes the deletion of the personal data and requests the restriction of processing instead; or

(iii) The agency no longer needs the personal data for the purposes of the processing, but the personal data is required by the consumer for the establishment, exercise, or defense of legal claims.

(g)(i) Where personal data is subject to a restriction of processing, the personal data should, with the exception of storage, only be processed: (A) With the consumer's consent; (B) for the

establishment, exercise, or defense of legal claims; (C) for the protection of the rights of another natural or legal person; or (D) for reasons of important public interest under federal, state, or local law;

(ii) A consumer who has obtained restriction of processing pursuant to this subsection should be informed by the agency before the restriction of processing is lifted.

(h) Agencies should provide the consumer, if technically feasible and commercially reasonable, any personal data that the agency maintains in identifiable form concerning a consumer that the consumer has provided to an agency in a structured, commonly used, and machine-readable format if: (i)(A) The processing of such personal data is necessary for the performance of a contract to which the consumer is a party or (B) 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.

(i) Agencies should communicate any correction, deletion, or restriction of processing carried out in accordance with this section to each third-party recipient to whom the agency knows personal data has been disclosed, including third parties that received the data through a sale, unless this proves functionally impractical, technically infeasible, or involves disproportionate effort.

(j) Agencies should provide information on action taken on a request under this section without undue delay and in any event within thirty days of receipt of the request.

(k) Agencies should provide information under this section by the agency free of charge to the consumer.

(5) This section expires June 1, 2021.

NEW SECTION. **Sec. 7.** A new section is added to chapter 43.105 RCW to read as follows:

(1) State agencies 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, meaningful privacy notice that includes:

(a) The categories of personal data collected by the state agency;

(b) The purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) The rights that consumers may exercise pursuant to section 5 of this act, if any;

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

(e) The categories of third parties, if any, with whom the state agency shares personal data.

(2) State agencies that engage in profiling must disclose such profiling to the consumer at or before the time personal data is obtained, including meaningful information about the logic involved and the significance and envisioned consequences of the profiling.

NEW SECTION. **Sec. 8.** A new section is added to chapter 43.105 RCW to read as follows:

(1) State agencies must certify compliance with the requirements of this chapter.

(2) By June 30, 2021, the office of privacy and data protection must provide a design template for consumer access to data and develop compliance criteria to meet the requirements of this chapter.

(3) This chapter applies to all state agencies. Agencies may request a waiver for hardship or inability to comply for special circumstances. The office of privacy and data protection must determine the waiver and must not unreasonably withhold it. The waiver may take the form of an extension of time to comply with specific provisions.

--- END ---