THE SENATE
THIRTY-THIRD LEGISLATURE, 2026
STATE OF HAWAII

S.B. NO. 3015 S.D. 1

A BILL FOR AN ACT

RELATING TO PERSONAL INFORMATION.

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

SECTION 1. The legislature finds that personally identifiable information maintained by government entities is increasingly targeted for exfiltration and misuse for financial fraud, identity theft, and other cybersecurity harms. The legislature further finds that definitions of personally identifiable information in State law are fragmented across chapters and, for certain government entities, do not reflect current technological realities, including the publication and indexing of government records through websites, searchable databases, bulk-download repositories, and application programming interfaces.

The legislature also finds that modern artificial intelligence systems may treat government records and databases as trusted sources and may be trained on, summarize, or generate content derived from those records. When personal information is publicly accessible through government systems, artificial

intelligence tools may inadvertently reproduce that information, compounding privacy, safety, and cybersecurity risks.

Accordingly, the purpose of this Act is to modernize and standardize protections for personal information maintained by government entities by:

(1) Prohibiting government entities from making personal information publicly accessible through a publicly accessible information system or publicly accessible source of information, except under certain conditions;

(2) Allowing individuals who reasonably believe their personal information is publicly accessible through a government entity's publicly accessible information system or publicly accessible source of information to submit a written notice to the entity to require corrective action;

(3) Establishing a cause of action to compel compliance;

(4) Establishing statutory penalties for intentional noncompliance;

(5) Requiring government entities to adopt and implement policies and procedures to prevent personal information from being publicly accessible;

(6) Requiring government entities that own, license, maintain, use, collect, or possess personal information to implement and maintain certain reasonable security procedures and practices to protect the personal information;

(7) Requiring government entities to provide notice to individuals in the case of a breach of a security system protecting personal information; and

(8) Requiring government entities to submit annual reports to the legislature.

SECTION 2. Chapter 84, Hawaii Revised Statutes, is amended by adding a new part to be appropriately designated and to read as follows:

"**PART . PERSONAL INFORMATION; GOVERNMENT INFORMATION SECURITY**

§84-A Definitions. As used in this part:

"Government entity" means any department, agency, board, commission, authority, or instrumentality of the State or a

county, including the legislature and its agencies, the judiciary and its administrative agencies, the office of Hawaiian affairs, and any public corporation or other establishment owned, operated, or managed by or on behalf of the State or any county.

"Genetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material.

"Health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

"Medical information" means any individually identifiable information, in electronic or physical form, regarding an individual's medical history or medical treatment or diagnosis by a health care professional.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more

of the following data elements, where either the name or the data elements are not encrypted or redacted:

(1) Social security number;

(2) Driver's license number, state identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;

(3) Account number, credit card number, or debit card number;

(4) Medical information;

(5) Health insurance information;

(6) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual; provided that unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes;

(7) Genetic data; and

(8) A username or electronic mail address in combination with a password or security question and answer that would permit access to an online account.

"Publicly accessible information system" means any website, portal, online searchable database, bulk-download repository, application programming interface, or substantially similar system that is made available to the public by a government entity without individualized authorization.

"Publicly accessible source of information" includes any document, record, image, dataset, or other information that is posted, published, indexed, or otherwise made available to the public through a publicly accessible information system.

"Redact" means to remove or obscure personal information so that it is not readable, not retrievable, and not usable by the public.

"Reasonable security procedures and practices" means security procedures and practices appropriate to the nature of the personal information, consistent with section 84-I.

§84-B Public posting of personal information; prohibition; publicly accessible information systems. (a) A government entity shall not make personal information publicly accessible

through a publicly accessible information system or publicly accessible source of information unless a federal or state statute, a rule adopted pursuant to statute, or a court order explicitly requires that the specific item of personal information be made publicly accessible.

(b) The obligation to disclose a government record under chapter 92F or any other law shall not, by itself, be construed to require a government entity to make personal information publicly accessible through a publicly accessible information system.

(c) Nothing in this part shall be construed to limit disclosure of government records as required by law; provided that a government entity shall employ redaction or sanitization to prevent public accessibility of personal information through publicly accessible information systems unless explicitly required under subsection (a).

(d) With respect to account numbers, credit card numbers, and debit card numbers, a government entity shall not make publicly accessible any portion of the number, whether in full or in part, unless explicitly required under subsection (a); provided that a government entity may make publicly accessible a

truncated number consisting only of the last four digits when the truncated number is reasonably necessary to identify a transaction or account reflected in a government record and no other personal information is made publicly accessible in connection with the truncated number.

(e) Each government entity shall implement and maintain processes designed to reduce the inadvertent public accessibility of personal information, including controls over posting, indexing, bulk downloads, and application programming interfaces, and reasonable measures to detect and remediate inadvertent public accessibility in publicly accessible information systems.

(f) For the purposes of this section, "make publicly accessible" includes publishing, posting, displaying, indexing, enabling search, enabling bulk download, or otherwise providing public access through any publicly accessible information system or publicly accessible source of information, including in text, image, scanned document, portable document format file, or other file format.

§84-C Notice of publicly accessible personal information; acknowledgement; corrective action. (a) Any individual who

reasonably believes that the individual's personal information is publicly accessible through a publicly accessible information system or publicly accessible source of information controlled by a government entity may submit a written notice to the government entity identifying, to the extent reasonably practicable, the location of the publicly accessible personal information.

(b) Within three business days after receipt of a written notice under subsection (a), the government entity shall provide a written acknowledgement to the individual and shall commence corrective action.

(c) A government entity shall complete corrective action within thirty days after receipt of a written notice under subsection (a) by removing, redacting, or otherwise sanitizing the personal information so that it is not publicly accessible; provided that this section shall not require removal or redaction of information that is explicitly required to be publicly accessible under section 84-B(a).

(d) Corrective action under this section shall be limited to the minimum necessary to remove public accessibility of the

personal information and shall not require deletion of non-personal information.

§84-D Extension of time to complete corrective action. A government entity that receives a valid written notice pursuant to section 84-C and requires additional time to complete corrective action may extend the time to complete corrective action by providing written notice to the individual within three business days after receipt of the written notice. An extension under this section may be for up to an additional ten business days; provided that the extension shall not extend the thirty-day period under section 84-C.

§84-E Civil remedies. (a) After providing written notice under section 84-C and allowing the government entity thirty days to complete corrective action, an individual whose personal information remains publicly accessible in violation of this part may bring an action for injunctive relief in the circuit court of competent jurisdiction to compel compliance.

(b) If the court finds that the government entity intentionally refused to take corrective action after receipt of a valid written notice, the court may, in addition to injunctive relief, award:

(1) Statutory damages of not less than $1,000 and not more than $5,000 per instance of intentional refusal; and

(2) Reasonable attorneys' fees and costs.

(c) This section shall not be construed to create a cause of action for monetary damages for negligent failure to complete corrective action, except as provided in subsection (b).

§84-F Exceptions; construction. (a) This part shall not apply to personal information that an individual voluntarily publishes on the Internet after the effective date of this Act.

(b) This part shall not be construed to require removal or redaction of information that is explicitly required to be publicly accessible under section 84-B(a).

(c) This part shall be construed to reduce public exposure of personal information through publicly accessible information systems while preserving access to government records as provided by law.

§84-G Policies; internal controls. Each government entity shall adopt and implement policies and procedures necessary to comply with this part, including policies governing public posting, redaction, sanitization, access controls for publicly accessible information systems, and incident response.

§84-H Government records. (a) Nothing in this part shall be construed to alter rights to access government records under chapter 92F or any other law.

(b) When a government entity discloses government records through a publicly accessible information system, the government entity shall not make personal information publicly accessible unless explicitly required under section 84-B(a).

§84-I Reasonable security procedures and practices; contractors; incident reporting. (a) A government entity that owns, licenses, maintains, uses, collects, or possesses personal information about an individual shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(b) A government entity that discloses personal information to a contractor or other third party for the purpose of performing services on behalf of the government entity shall require, by contract, that the contractor or third party:

(1) Implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information;

(2) Report any breach of the security of the system, or suspected breach involving personal information, to the government entity as soon as practicable, but in no event later than seventy-two hours after discovery;

(3) Cooperate with investigation, containment, and notification obligations;

(4) Require the same or substantially similar obligations to be imposed on subcontractors or subservice providers;

(5) Provide, upon request, reasonable assurances of compliance, including audit rights or independent attestations aligned with commonly accepted security frameworks, including Systems and Organizations Controls 2 (SOC 2) or National Institute of Standards and Technology (NIST)-based controls; and

(6) Minimize the personal information processed for the contract and, upon completion or termination of the contract, return or securely destroy personal

information, subject to any legal retention requirements.

§84-J Breach of security of system; notice. (a) In the case of a breach of the security of the system involving personal information, a government entity that owns or licenses computerized data that includes personal information shall disclose the breach following discovery or notification of the breach to any resident of the State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

(b) Notification may be delayed if a law enforcement agency determines that notification will impede a criminal investigation. Notification shall be made promptly after the law enforcement agency determines that notification will not compromise the investigation.

(c) The notification required by this section shall be written in plain language, titled "Notice of Data Breach", and present the information under the following headings:

(1) "What Happened?";

(2) "What Information Was Involved?";

(3) "What We Are Doing.";

(4) "What You Can Do."; and

(5) "For More Information.".

(d) The notification required by this section shall include, at a minimum:

(1) The name and contact information of the reporting government entity;

(2) A list of the types of personal information that were, or are reasonably believed to have been, the subject of a breach;

(3) If available at the time of notice, the date of the breach, the estimated date of the breach, or the date range within which the breach occurred;

(4) Whether notification was delayed as a result of a law enforcement investigation;

(5) A general description of the breach incident, described in a manner that does not compromise security controls;

(6) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed information that could be used for identity theft; and

(7) If the breach exposed a social security number or a driver's license or state identification card number, advice to the affected individual to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) Notice under this section may be provided by written notice, electronic notice if consistent with applicable law, or substitute notice if the government entity demonstrates that the cost of providing notice would exceed an amount specified by rule or that the affected class of persons to be notified exceeds a number specified by rule; provided that substitute notice shall include, at a minimum, email notice when available, conspicuous posting on the government entity's website, and notification to major statewide media.

(f) A government entity shall maintain records of breaches and notices provided under this section for five years.

(g) For the purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the government entity; provided that good faith acquisition of personal information by an employee or agent of the government entity for the purposes of the government entity is not a breach of the security of the system; provided further that the personal information is not used or subject to further unauthorized disclosure.

§84-K Compliance with this part; annual reporting requirement. Each government entity shall submit an annual report detailing compliance with this part to the legislature no later than twenty days prior to the convening of each regular session.

§84-L Office of Hawaiian affairs, public corporations, and other establishments; applicability of part. For the office of Hawaiian affairs, public corporations, and other establishments, the requirements of this part shall apply only to publicly

accessible information systems and publicly accessible sources of information."

SECTION 3. Chapter 92H, Hawaii Revised Statutes, is amended by adding a new section to be appropriately designated and to read as follows:

"**§92H- Relationship to part of chapter 84.** Nothing in this chapter shall be construed to limit or impair the requirements of part of chapter 84."

SECTION 4. Chapter 84, Hawaii Revised Statutes, is amended by amending its title to read as follows:

"**CHAPTER 84**

STANDARDS OF CONDUCT; GOVERNMENT INFORMATION SECURITY"

SECTION 5. In codifying the new sections added by section 2 of this Act, the revisor of statutes shall substitute appropriate section numbers for the letters used in designating the new sections in this Act.

SECTION 6. New statutory material is underscored.

SECTION 7. This Act shall take effect on January 1, 2525.

S.B. NO. 3015 S.D. 1

Report Title:
Personal Information; Government Entities; Publicly Accessible Information Systems; Publication Controls; Data Security; Notification; Cause of Action; Reports

Description:
Prohibits government entities from making personal information publicly accessible through a publicly accessible information system or publicly accessible source of information, except under certain conditions. Allows individuals who reasonably believe their personal information is publicly accessible through a government entity's publicly accessible information system or publicly accessible source of information to submit a written notice to the entity to require corrective action. Establishes a cause of action to compel compliance. Establishes statutory penalties for intentional noncompliance. Requires government entities to adopt and implement policies and procedures to prevent personal information from being publicly accessible. Requires government entities that own, license, maintain, use, collect, or possess personal information to implement and maintain certain reasonable security procedures and practices to protect the personal information. Requires government entities to provide notice to individuals in the case of a breach of a security system protecting personal information. Requires government entities to submit an annual report to the Legislature. Effective 1/1/2525. (SD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.