AMENDED IN ASSEMBLY MAY 1, 2015

AMENDED IN ASSEMBLY APRIL 16, 2015

AMENDED IN ASSEMBLY APRIL 9, 2015

AMENDED IN ASSEMBLY MARCH 26, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 739

Introduced by Assembly Member Irwin

February 25, 2015

An act to add and repeal Section 43.99.1 to the Civil Code, relating to civil law.

LEGISLATIVE COUNSEL'S DIGEST

AB 739, as amended, Irwin. Civil law: liability: communication of cyber ~~security: threat~~ *security-threat* information.

Existing law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law requires a person or business conducting business in California that owns or licenses computerized data that includes personal information, as defined, to disclose, as specified, a breach of the security of the system or data following discovery or notification of the security breach to any California resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, unless the information was encrypted. Existing law also requires a person or business that maintains computerized data that includes

personal information that the person or business does not own to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, as specified.

This bill would, until January 1, 2020, provide that there shall be no civil or criminal liability for, and no cause of action shall ~~arise against, an~~ *lie or be maintained against any private* entity ~~based upon its communication of cyber security-threat information to another private entity, or to a state law enforcement agency.~~ *for the sharing or receiving of cyber security-threat information if the sharing or receiving is conducted, as specified.* The immunity from liability would only apply if the communication is made without ~~the intent to injure, defraud, or to otherwise endanger any individual or public or private entity and is made to address a vulnerability in, or to prevent a threat to the integrity, confidentiality, or availability of, a system, network, or critical infrastructure component of a public or private entity, to provide support for cyber security crime investigation, or to protect individuals, entities, or the state from harm,~~ *gross negligence,* as specified. The bill would also prohibit a private entity that ~~communicates~~ *is engaged in sharing or receiving* cyber security-threat information from using that information to gain an unfair competitive advantage and require that it, in good faith, make reasonable efforts to safeguard communications, comply with any lawful restriction placed on the communication, transfer the cyber security-threat information as expediently as possible while upholding reasonable protections, and ensure that appropriate anonymization and minimization of the information contained in the communication, as specified.

~~This bill would specify that a communication of cyber security-threat information made in compliance with this section and shared with a public agency is confidential and shall not be disclosed under the California Public Records Act.~~

~~Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.~~

~~This bill would make legislative findings to that effect.~~

Vote: majority. Appropriation: no. Fiscal committee: ~~yes~~ *no*. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 43.99.1 is added to the Civil Code, to read:

43.99.1. (a) ~~There shall be no civil or criminal liability for, and no~~ *(1) No* cause of action shall ~~arise~~ *lie, or be maintained* against, ~~a~~ *any* private entity ~~whose actions comply~~ *for the sharing or receiving of cyber security-threat information if the sharing or receiving is conducted in accordance* with subdivision (b) based upon its communication of cyber security-threat information to another private ~~entity, or to a state law enforcement agency.~~ *or public entity.* The immunity from liability granted by this section shall only apply if the communication is made without ~~the intent to injure, defraud, or to otherwise endanger any individual or public or private entity and is made for one of the following purposes:~~ *gross negligence.*

~~(1) To address a vulnerability of a system, network, or critical infrastructure component of a public or private entity.~~

~~(2) To prevent a threat to the integrity, confidentiality, or availability of a system, network, or critical infrastructure component of a public or private entity.~~

~~(3) To provide support for cyber security crime investigation.~~

~~(4) To protect individuals and entities from personal or economic harm.~~

~~(5) To protect the state's economic interests, including, but not limited to, networks, assets, and personal information.~~

(2) Nothing in this subdivision shall be construed to require dismissal of a cause of action against a private entity that has engaged in gross negligence in the course of sharing or receiving cyber security-threat information, or to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(3) In any action claiming that the immunity from liability described in paragraph (1) does not apply due to the defendant acting with gross negligence, the plaintiff shall have the burden of proving by substantial evidence the gross negligence and that the gross negligence caused injury to the plaintiff.

(4) For purposes of this section, "gross negligence" includes actions that include all of the following elements engaged in:

(A) To intentionally injure, defraud, or otherwise endanger any individual or public or private entity.

(B) Knowingly without legal or factual justification.

(C) Without regard for a foreseeable risk that is so great as to make it highly probable that the harm will outweigh the benefit.

(D) Involving information that serves as criminal evidence for matters unrelated to a cyber security-threat or the otherwise known business of the private entity.

(b) A private entity that ~~communicates~~ *is engaged in sharing or receiving* cyber security-threat information shall not use that information to gain an unfair competitive advantage and shall, in good faith, do all of the following:

(1) Make reasonable efforts to safeguard communications that can be used to identify specific persons from unauthorized access or acquisition.

(2) Comply with any lawful restriction placed on the communication, including the removal of information that can be used to identify specific persons.

(3) Transfer the cyber security-threat information as expediently as possible while upholding reasonable protections.

(4) Ensure, at a minimum, appropriate anonymization and minimization of the information contained in the communication.

(c) For purposes of this section, "cyber security-threat information" means information pertaining directly to one of the following:

(1) A vulnerability of a system, network, or critical infrastructure component of a public or private entity.

(2) A threat to the integrity, confidentiality, or availability of a system, network, or critical infrastructure component of a public or private entity.

(3) Efforts to deny access to, or to cause the degradation, disruption, or destruction of a system, network, or critical infrastructure component of a public or private entity.

(4) Efforts to gain unauthorized access to a system, network, or critical infrastructure component of a public or private entity, including efforts to gain unauthorized access for the purpose of exfiltrating information stored on, processed on, or transitioning through, a system, network, or critical infrastructure component of a public or private entity.

~~(d) A communication of cyber security-threat information made in compliance with this section and shared with a public agency is confidential and shall not be disclosed under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1 of the Government Code).~~

~~(e)~~

(d) This section shall become inoperative on January 1, 2020, and as of that date is repealed.

~~SEC. 2. The Legislature finds and declares that Section 1 of this act, which adds Section 6254.32 to the Government Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:~~

~~The need to protect information regarding the specific vulnerabilities of and threats to information technology systems to preclude use of that information to facilitate attacks on those systems outweighs the interest in the public disclosure of that information.~~

O