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 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 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 require the Attorney General to create a registry of private entities that intend to engage in communication of cyber security-threat information, as defined. The bill would also provide that there shall be no civil or criminal liability for, and no cause of action shall arise against, a registered entity based upon its communication of cyber security-threat information to another private entity, or to a state entity. 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 or the state from harm, as specified. *The bill would also prohibit a private entity that communicates cyber security-threat information from using that information to gain an unfair competitive advantage and require that it make reasonable efforts to safeguard communications, comply with any lawful restriction placed on the communication, and transfer the cyber security-threat information as expediently as possible while upholding reasonable protections, as specified.*

The bill would also require the Attorney General to submit an annual report to the Legislature regarding the operation of these provisions that includes an assessment of the impact of these provisions on the privacy of the personal information of California residents.

Vote: majority. Appropriation: no. Fiscal committee: yes. 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 cause of action shall arise against, a private entity *whose actions comply with subdivision (b), and* that has registered with the Attorney General pursuant to subdivision ~~(b),~~ *(c)*, based upon its communication of cyber security-threat information to another private entity, or to a state entity identified by the Attorney General. 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:

(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 from personal or economic harm.

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

(b) A private entity that communicates cyber security-threat information shall not use that information to gain an unfair competitive advantage and shall 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.

~~(b)~~

(c) The Attorney General shall create a registry of private entities that intend to engage in communication of cyber security-threat information.

(d) The Attorney General shall submit an annual report to the Legislature regarding the operation of these provisions that includes an assessment of the impact of these provisions on the privacy of the personal information of California residents.

~~(c)~~

(e) 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.

(f) (1) The requirement for submitting a report imposed under subdivision (d) is inoperative on January 1, 2020, pursuant to Section 10231.5 of the Government Code.

(2) A report to be submitted pursuant to subdivision (d) shall be submitted in compliance with Section 9795 of the Government Code.

O