AMENDMENT TO THE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 8152

OFFERED BY MR. Hudson and Mr. O'Halleran

Page 98, after line 9, add the following new section:

SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

(1) shall adhere to the instructions of a covered entity and only collect, process, and transfer service provider data to the extent necessary and proportionate to provide a service requested by the covered entity, as set out in the contract required by subsection (b), and this paragraph does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

(2) may not collect, process, or transfer service provider data if the service provider has actual knowledge that a covered entity violated this Act with respect to such data;

(3) shall assist a covered entity in responding to a request made by an individual under section 203 or 204, by either—

(A) providing appropriate technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the service provider, for the covered entity to comply with such request for service provider data; or

(B) fulfilling a request by a covered entity to execute an individual rights request that the covered entity has determined should be complied with, by either—

(i) complying with the request pursuant to the covered entity's instructions; or

(ii) providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception to section 203 or 204;

(4) may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing that covered entity with notice and pursuant to a written contract that requires such other service provider to satisfy the obligations of the service provider with

respect to such service provider data, including that the other service provider be treated as a service provider under this Act;

(5) shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the compliance of the service provider with the requirements of this Act, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the service provider and the covered entity, providing information necessary to enable the covered entity to conduct and document a privacy impact assessment required by subsection (d) or (e) of section 301, and making available the report required under section 207(c)(2);

(6) shall, at the covered entity's direction, delete or return all covered data to the covered entity as requested at the end of the provision of services, unless retention of the covered data is required by law;

(7) shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and

confidentiality of covered data the service provider processes consistent with section 208; and

(8) shall allow and cooperate with, reasonable assessments by the covered entity or the covered entity's designated assessor; alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the service provider's policies and technical and organizational measures in support of the obligations under this Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The service provider shall provide a report of such assessment to the covered entity upon request.

(b) CONTRACTS BETWEEN COVERED ENTITIES AND SERVICE PROVIDERS.—

(1) REQUIREMENTS.—A person or entity may only act as a service provider pursuant to a written contract between the covered entity and the service provider, or a written contract between one service provider and a second service provider as described under subsection (a)(4), if the contract—

(A) sets forth the data processing procedures of the service provider with respect to col-

lection, processing, or transfer performed on behalf of the covered entity or service provider;

(B) clearly sets forth—

(i) instructions for collecting, processing, or transferring data;

(ii) the nature and purpose of collecting, processing, or transferring;

(iii) the type of data subject to collecting, processing, or transferring;

(iv) the duration of processing; and

(v) the rights and obligations of both parties, including a method by which the service provider shall notify the covered entity of material changes to its privacy practices;

(C) does not relieve a covered entity or a service provider of any requirement or liability imposed on such covered entity or service provider under this Act; and

(D) prohibits—

(i) collecting, processing, or transferring covered data in contravention to subsection (a); and

(ii) combining service provider data with covered data which the service pro-

vider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, provided that such combining is not necessary to effectuate a purpose described in paragraphs (1) through (15) of section 101(b) and is otherwise permitted under the contract required by this subsection.

(2) CONTRACT TERMS.—Each service provider shall retain copies of previous contracts entered into in compliance with this subsection with each covered entity to which it provides requested products or services.

(c) RELATIONSHIP BETWEEN COVERED ENTITIES AND SERVICE PROVIDERS.—

(1) Determining whether a person is acting as a covered entity or service provider with respect to a specific processing of covered data is a fact-based determination that depends upon the context in which such data is processed.

(2) A person that is not limited in its processing of covered data pursuant to the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and not a service

provider with respect to a specific processing of covered data. A service provider that continues to adhere to the instructions of a covered entity with respect to a specific processing of covered data remains a service provider. If a service provider begins, alone or jointly with others, determining the purposes and means of the processing of covered data, it is a covered entity and not a service provider with respect to the processing of such data.

(3) A covered entity that transfers covered data to a service provider or a service provider that transfers covered data to a covered entity or another service provider, in compliance with the requirements of this Act, is not liable for a violation of this Act by the service provider or covered entity to whom such covered data was transferred, if at the time of transferring such covered data, the covered entity or service provider did not have actual knowledge that the service provider or covered entity would violate this Act.

(4) A covered entity or service provider that receives covered data in compliance with the requirements of this Act is not in violation of this Act as a result of a violation by a covered entity or service provider from which such data was received.

(d) THIRD PARTIES.—A third party—

(1) shall not process third party data for a processing purpose other than, in the case of sensitive covered data, the processing purpose for which the individual gave affirmative express consent or to effect a purpose enumerated in paragraph (1), (3), or (5) of section 101(b) and, in the case of non-sensitive data, the processing purpose for which the covered entity made a disclosure pursuant to section 202(b)(4); and

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third party data if the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible.

(e) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES.—

(1) IN GENERAL.—A covered entity or service provider shall exercise reasonable due diligence in—

(A) selecting a service provider; and

(B) deciding to transfer covered data to a third party.

(2) GUIDANCE.—Not later than 2 years after the date of enactment of this Act, the Commission

shall publish guidance regarding compliance with this subsection, taking into consideration the burdens on large data holders, covered entities who are not large data holders, and covered entities meeting the requirements of section 209.

(f) RULE OF CONSTRUCTION.—Solely for the purposes of this section, the requirements for service providers to contract with, assist, and follow the instructions of covered entities shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the service provider is providing a service to a government entity.

Page 98, line 10, strike "**302**" and insert "**303**".

Page 101, line 10, strike "**303**" and insert "**304**".

Page 106, line 3, strike "**304**" and insert "**305**".

☒