Side-by-Side of Key Legislative Text
Cantwell and Three Corners Privacy Drafts
June 6, 2022

Side-by-side text and summaries of major provisions of Sen. Cantwell and Three Corner federal privacy discussion drafts.

CONTENTS

Key Definitions 2
Key Obligations 11
CORPORATE ACCOUNTABILITY 42
Enforcement 53
Preemption 67

KEY DEFINITIONS

Cantwell	Cantwell Amendment	Three Corners
(1) AFFIRMATIVE EXPRESS CONSENT. —	(1) AFFIRMATIVE EXPRESS CONSENT. —	(1) AFFIRMATIVE EXPRESS CONSENT. —
(A) IN GENERAL. —The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's authorization for an act or practice, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).	(A) IN GENERAL. —The term ''affirmative express consent'' means an affirmative act by an individual that clearly communicates the individual's authorization for an act or practice, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).	(A)IN GENERAL. —The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's **freely given, specific, informed, and unambiguous** authorization for an act or practice, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).
(B) REQUEST REQUIREMENTS. — The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:	(B) REQUEST REQUIREMENTS. — The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:	(B) REQUEST REQUIREMENTS. — The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:
(i) The request is provided to the individual in a standalone disclosure.	(i) The request is provided to the individual in a standalone disclosure.	(i) The request is provided to the individual in a **clear and conspicuous** standalone disclosure **made through the primary medium used to offer the covered entity's product or service**.
(ii) The request includes a description of each act or practice for which the individual's consent is sought and—	(ii) The request includes a description of each act or practice for which the individual's consent is sought and—	(ii) The request includes a description of each act or practice for which the individual's consent is sought and—
(I) clearly distinguishes between an act or practice which is necessary to fulfill a request of the individual and an act or practice which is for another purpose; and	(I) clearly distinguishes between an act or practice which is necessary to fulfill a request of the individual and an act or practice which is for another purpose; and	**(I) clearly states the specific types of covered data that the covered entity shall collect, process, or transfer for each act or practice**;
(II) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable individual to identify and understand the act or practice.	(II) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable individual to identify and understand the act or practice.	(II) clearly distinguishes between any act or practice which is necessary to fulfill a request of the individual and **any** act or practice which is for another purpose; and
	(iii) The request clearly explains the individual's applicable rights related to consent.	(III) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable individual to identify and understand the act or practice **and the covered data to be collected, processed, or**
(iii) The request clearly explains the individual's applicable rights related to consent.	(C) EXPRESS CONSENT REQUIRED. —An entity shall not	

(C) EXPRESS CONSENT REQUIRED. —An entity shall not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the entity.	infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the entity.	**transferred by the covered entity for such act or practice**. (iii) The request clearly explains the individual's applicable rights related to consent. **(iv) The request shall be made available to the public in each language in which the covered entity provides a product or service for which authorization is sought or in which the covered entity carries out any activity related to any product or service the covered data of the individual may be collected, processed, or transferred.** (C) EXPRESS CONSENT REQUIRED. —A **covered** entity shall not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the entity. **(D)PRETEXTUAL CONSENT PROHIBITED. —A covered entity shall not obtain or attempt to obtain the affirmative express consent of an individual through—** **(i) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or** **(ii) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data.**
Notes: Substantially similar definitions, but Three Corners goes further by putting in more technical detail and prohibiting "pretextual" methods of obtaining consent, aiming to restrict dark patterns.		

Cantwell	**Cantwell Amendment**	**Three Corners**

(4) COLLECT, COLLECTION. —The terms “collect” and “collection” mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means	(4) COLLECT, COLLECTION. —The terms ‘‘collect’’ and ‘‘collection’’ mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.	(4) COLLECT, COLLECTION. —The terms “collect” and “collection” mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.
Notes: Identical definitions.		

Cantwell	**Cantwell Amendment**	**Three Corners**
(8) COVERED DATA. — (A) IN GENERAL. —The term “covered data” means information that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals, including derived data and unique identifiers. (B) EXCLUSIONS. —The term “covered data” does not include— (i) de-identified data; (ii) employee data; or (iii) publicly available information.	(8) COVERED DATA. — (A) IN GENERAL. —The term ‘‘covered data’’ means information that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals, including derived data and unique identifiers. (B) EXCLUSIONS. —The term ‘‘covered data’’ does not include— (i) de-identified data; (ii) employee data; or (iii) publicly available information.	(8) COVERED DATA. — (A) IN GENERAL. —The term “covered data” means information that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals, including derived data and unique identifiers. (B) EXCLUSIONS. —The term “covered data” does not include— (i) de-identified data; (ii) employee data; or (iii) publicly available information. **(C) EMPLOYEE DATA DEFINED. —For purposes of subparagraph (B), the term “employee data” means—** **(i) information relating to a prospective employee collected by a covered entity acting as a prospective employer of such prospective employee in the course of the application or hiring process, provided that such information is collected, processed, or transferred by the prospective employer solely for purposes related to the employee’s status as a current or former job applicant of such employer;** **(ii) the business contact information of an employee, including the employee’s name, position or title, business telephone number, business address, or business email address that is provided to an employer by an employee who is acting in a**

		professional capacity, provided that such information is collected, processed, or transferred solely for purposes related to such employee's professional activities; **(iii) emergency contact information collected by an employer that relates to an employee of that employer, provided that such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the employee; or** **(iv) information relating to an employee (or a relative or beneficiary of such employee) that is necessary for the employer to collect, process, or transfer solely for the purpose of administering benefits to which such employee (or relative or beneficiary of such employee) is entitled on the basis of the employee's position with that employer.**
Notes: Covered data is any information linked or linkable to an individual or device. Includes inferences and derived data. Identical except Three Corners explicitly defines Employee Data.		

Cantwell	**Cantwell Amendment**	**Three Corners**
(9) COVERED ENTITY. —The term "covered entity"— (A) means any entity or person that processes or transfers covered data and— (i) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); [(ii) is a common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended; or] (iii) is an organization not organized to carry on business for their own profit or that of their members; and (B) includes any entity or person that controls, is controlled by, is under common control with, or shares	(9) COVERED ENTITY. —The term ''covered entity''— (A) means any entity or person that processes or transfers covered data and— (i) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); (ii) is a common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended; or (iii) is an organization not organized to carry on business for their own profit or that of their members; and (B) includes any entity or person that controls, is controlled by, is under common control with, or shares	(9) COVERED ENTITY. —The term "covered entity"— (A)means any entity or person that **collects**, processes, or transfers covered data and— (i)is subject to the Federal Trade Commission Act (15U.S.C. 41 et seq.); (ii) is a common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended; or (iii)is an organization not organized to carry on business for their own profit or that of their members; and (B) includes any entity or person that controls, is controlled by, is under common control with, or shares

common branding with another covered entity.	common branding with another covered entity.	common branding with another covered entity.
Notes: Cantwell defines as any entity that processes or transfers covered data and is subject to FTC jurisdiction, is a common carrier, or is a nonprofit. Three Corners is the same except that collecting data is also a trigger for coverage.		

Cantwell	**Cantwell Amendment**	**Three Corners**
(16) LARGE DATA HOLDER. —The term "large data holder" means a covered entity that, in the most recent calendar year—	(14) LARGE DATA HOLDER. —The term ''large data holder'' means a covered entity that, in the most recent calendar year—	(17) LARGE DATA HOLDER. —The term "large data holder" means a covered entity that, in the most recent calendar year— **(A)had annual gross revenues of [$250,000,000] or more; [and]**
(A) processed or transferred the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals; or (B) processed or transferred the sensitive covered data of more than 100,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding any instance where the covered entity would qualify as a large data holder solely on account of processing—	(A) processed or transferred the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals; or (B) processed or transferred the sensitive covered data of more than 100,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding any instance where the covered entity would qualify as a large data holder solely on account of processing—	(B) **collected**, processed, or transferred— (i)the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals: **[**or**]** (ii)the sensitive covered data of more than **[**100,000] individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding any instance where the covered entity would qualify as a large data holder solely on account of processing—
(i) personal email addresses; (ii) personal telephone numbers; or (iii) log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity.	(i) personal email addresses; (ii) personal telephone numbers; or (iii) log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity.	(I) personal email addresses; (II) personal telephone numbers; or (III) log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity.
Notes: Cantwell defines as a covered entity that also processed or transferred covered data of more than 5 million individuals or devices in a year or the same for the sensitive information of 100,000 individuals or devices. Three Corners further includes a revenue threshold of $250 million and allows collection of data as a trigger.		

Cantwell	**Cantwell Amendment**	**Three Corners**
(21) SERVICE PROVIDER. —	(19) SERVICE PROVIDER. —	(23) SERVICE PROVIDER. —

(A) IN GENERAL. —The term "service provider" means a covered entity that processes, or transfers covered data in the course of performing 1 or more services or functions on behalf of, and at the direction of, another covered entity, but only to the extent that such processing or transfer— (i) relates to the performance of such service or function; or (ii) is necessary to comply with a legal obligation or to establish, exercise, or defend legal claims. (B) EXCLUSION. —The term "service provider" does not include a covered entity that processes, or transfers covered data outside of ~~the~~ direct relationship between the service provider and the covered entity as described in subparagraph (A).	(A) IN GENERAL. —The term ''service provider'' means a covered entity that processes or transfers covered data in the course of performing 1 or more services or functions on behalf of, and at the direction of, another covered entity, but only to the extent that such processing or transfer— (i) relates to the performance of such service or function; or (ii) is necessary to comply with a legal obligation or to establish, exercise, or defend legal claims. (B) EXCLUSION. —The term ''service provider'' does not include a covered entity that processes or transfers covered data outside of the direct relationship between the service provider and the covered entity as described in subparagraph (A).	(A) IN GENERAL. —The term "service provider" means a covered entity that **collects**, processes, or transfers covered data in the course of performing 1 or more services or functions on behalf of, and at the direction of, another covered entity, but only to the extent that such collection, processing, or transfer— (i) relates to the performance of such service or function; or (ii) is necessary to comply with a legal obligation or to establish, exercise, or defend legal claims. (B) EXCLUSION. —The term "service provider" does not include a covered entity **in so far as such covered entity collects**, processes, or transfers covered data outside of **a** direct relationship between the service provider and the covered entity as described in subparagraph (A).
Notes: This is a problematic definition because it makes service providers a subcategory of covered entities, rather than creating a separate category with different obligations. Any covered entity that processes or transfers data on behalf of another covered entity insofar as the actions the service provider takes are to perform the service for the other covered entity. Three Corners includes collection on behalf of a covered entity as a trigger.		

Cantwell	**Cantwell Amendment**	**Three Corners**
(23) SUBSTANTIAL PRIVACY HARM—The term "substantial privacy harm" means: Alleged financial harm to an individual of $1000 or more, adjusted annually for inflation; (A) Alleged physical or mental harm to an individual that involves— (i) Treatment by a health care provider, hospital, community health center, clinic, hospice, or residential or	(21) SUBSTANTIAL PRIVACY HARM. —The term ''substantial privacy harm'' means— (A) an alleged harm, as further defined in subparagraphs (B) and (C), of $10,000 or more, adjusted annually for inflation; (B) an alleged financial harm; or (C) an alleged physical or mental harm to an individual that involves— (i) treatment by a licensed, credentialed, or otherwise bona fide healthcare provider, hospital, community health center, clinic,	--

outpatient facility for medical, mental health, or addiction care; or (ii) Injury from trauma or post-traumatic stress disorder brought on by physical injury, threat of death or severe harm, harassment, non-consensual touching of a sexual or physical nature, or false imprisonment; ~~(iii) A reasonable expectation of anticipated physical harm based on specific facts and circumstances alleged at the time of injury;~~ ~~(B) An alleged intrusion upon the seclusion of an individual arising from the collection, processing, or transfer of —~~ ~~(i) Any information that describes or reveals the past, present, or future physical health, mental health, genetic information, disability, diagnosis, or healthcare treatment of an individual;~~ ~~(ii) That is collected, processed, or transferred by a covered entity that is not required to comply with the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.); and~~ ~~(iii)The intrusion would be considered offensive to a reasonable person; or~~ ~~(C) Alleged harm to the reputation of an individual such as to lower the individual in the estimation of the community or deter others from associating or dealing with the individual.~~	hospice, or residential or outpatient facility for medical, mental health, or addiction care; or (ii) injury from trauma or post-traumatic stress disorder brought on by physical injury, threat of death or severe harm, harassment, non-consensual touching of a sexual or physical nature, non-consensual sexual images, or false imprisonment.	
Notes: Not included in Three Corners. Substantial Privacy Harm is any that involves over $1,000 of financial harm, or serious physical or mental harm. Also includes serious intrusion upon seclusion of an individual. These types of harms would not be subject to arbitration in Cantwell's bill.		

Cantwell	**Cantwell Amendment**	**Three Corners**

(25) THIRD PARTY. —The term "third party"— (A) means any person or entity that— (i) processes or transfers third party data; and (ii) is not a service provider with respect to such data; and (B) does not include a person or entity that collects covered data from another entity if the 2 entities are related by common ownership or corporate control and share common branding.	(23) THIRD PARTY. —The term ''third party''— (A) means any person or entity that— (i) processes or transfers third party data; and (ii) is not a service provider with respect to such data; and (B) does not include a person or entity that collects covered data from another entity if the entities are related by common ownership or corporate control and share common branding.	(27) THIRD PARTY. —The term "third party"— (A)means any person or entity that— (i) **collects,** processes, or transfers third party data; and (ii) is not a service provider with respect to such data; and (B) does not include a person or entity that collects covered data from another entity if the 2 entities are related by common ownership or corporate control and share common branding, **unless one of those is a large data holder or those entities are each related by common ownership or corporate control with respect to a large data holder**.
	Notes: Any person or entity other than a service provider that processes data. Cantwell excludes entities with common branding, while Three Corners includes commonly branded Large Data Holders.	

Cantwell	**Three Corners**
--	(28) THIRD-PARTY COLLECTING ENTITY. — (A) IN GENERAL. —The term "third-party collecting entity"— (i) means a covered entity whose principal source of revenue derived from processing or transferring the covered data of individuals that the covered entity did not collect directly from the individuals to which the covered data pertains; and (ii)does not include a covered entity in so far as such entity processes [information/employee data] collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third-party providing benefits to the employee. (B) PRINCIPAL SOURCE OF REVENUE DEFINED. —For purposes of this paragraph, "principal source of revenue" means, for the prior 12-month period, either (i) more than 50% of all revenue of the covered entity; or (ii) obtaining revenue from processing or transferring the covered data of more than 5,000,000 individuals that the covered entity did not collect directly from the individuals to which the covered data pertains.

	(C) NON-APPLICATION TO SERVICE PROVIDERS. — A covered entity shall not be considered to be a third-party collecting entity for purposes of this Act if the covered entity
Notes: Not included in Cantwell. Intended to cover data brokers. Covered if over 50% of revenue is from data entity didn't collect or processes data of 5 million individuals from whom it did not directly collect data.	

Cantwell	**Cantwell Amendment**	**Three Corners**
(27) TRANSFER. —The term "transfer" means to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any other means **for consideration of any kind or for a commercial purpose**.	(25) TRANSFER. —The term ''transfer'' means to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any other means for consideration of any kind or for a commercial purpose.	(30) TRANSFER. —The term "transfer" means to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any other means.
Notes: Any movement or availability of data. In Cantwell, restricted to commercial purposes only.		

KEY OBLIGATIONS

Cantwell	Cantwell Amendment	Three Corners
[SEC. 101 PROHIBITION ON DECEPTIVE AND HARMFUL DATA PRACTICES.] A covered entity shall not— [(1) engage in a deceptive data practice or a harmful data practice; or (2) process or transfer covered data in a manner that violates any provision of this Act.]	SEC. 101. DATA CARE. (a) IN GENERAL. —A covered entity shall not process or transfer covered data in a manner that will result in any reasonably foreseeable and material physical or financial harm to an individual. (b) ENFORCEMENT. —This section shall be enforced solely by the Commission in an action for injunctive relief brought in Federal district court, provided that such action is brought only following investigation and determination, by vote of the Commission, that the Commission has reason to believe a covered entity is violating, or is about to violate, the prohibition in subsection (a). Any violation of injunctive relief granted pursuant to this subsection shall be enforceable pursuant to paragraphs (1) and (2) of sections 401(b).	--
Notes: Applies to Covered Entities Prohibits deceptive or harmful practices as defined. Not included in Three Corners.		

Cantwell	Cantwell Amendment	Three Corners
SEC. 102. DATA MINIMIZATION. A covered entity shall not process or transfer covered data beyond— (1) what is reasonably necessary, proportionate, and limited to provide or maintain— (A) a specific product or service requested by an individual; or (B) a communication by the covered entity to the individual reasonably anticipated within the context of the relationship; or	SEC. 102. DATA MINIMIZATION. A covered entity shall not process, or transfer covered data beyond— (1) what is reasonably necessary, proportionate and limited to provide or maintain— (A) a specific product or service requested by an individual; or (B) a communication by the covered entity to the individual reasonably anticipated within the context of the relationship; or	SEC. 101. DATA MINIMIZATION. (a) IN GENERAL. —A covered entity shall not **collect**, process, or transfer covered data beyond what is reasonably necessary, proportionate, and limited to— (1) provide or maintain— (A) a specific product or service requested by an individual; or (B) a communication by the covered entity to the individual reasonably anticipated within the context of the relationship; or

(2) a purpose expressly permitted by this Act.	(2) a purpose expressly permitted by this Act.	(2) a purpose expressly permitted by this Act. **(b) GUIDANCE. —The Commission shall issue guidance to establish what is reasonably necessary, proportionate, and limited to comply with this section. Such guidance shall take into consideration—** **(1) the size of, and the nature, scope, and complexity of the activities engaged in by the covered entity, including whether the covered entity is a large data holder or third-party collecting entity;** **(2) the sensitivity of covered data collected, processed, or transferred by the covered entity;** **(3) the volume of covered data collected, processed, or transferred by the covered entity; and** **(4) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates**.
Notes: Applies to Covered Entities. Must only collect (Three Corners Only) process and transfer data as necessary and reasonable to provide services requested or expected by customer. Three Corners requires FTC to provide guidance on reasonability and compliance.		

Cantwell	**Three Corners**
--	SEC. 102. LOYALTY DUTIES. (a) RESTRICTED AND PROHIBITED DATA PRACTICES. —The following practices shall be restricted and prohibited: (1) The collection, processing, or transferring of social security numbers, except when necessary to facilitate extensions of credit, authentication, or the payment and collection of taxes. (2) The transfer of an individual's precise geolocation information to a third party, unless transferred to another device or service of such individual with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the

	precise geolocation information will be transferred with such a notice provided for each instance in which such transfer is to occur absent a search warrant or exigent circumstances. (3)The collection, processing, or transferring of biometric information, except for data security, authentication, to comply with a legal obligation, to establish, exercise, or defend a legal claim, for law-enforcement purposes, or with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the biometric information will be collected, processed, or transferred with such a notice provided for each instance in which such collection, processing, or transferring is to occur. (4) The transfer of any password, except when the transfer is made to a designated password manager, or a covered entity whose exclusive purpose is to identify passwords that are being re-used across sites or accounts, absent a search warrant or exigent circumstances. (5) The collection, processing, or transferring, of known nonconsensual intimate images, except for law enforcement purposes. (6) The collection, processing, or transferring of genetic information, except for purposes of medical diagnosis, medical treatment, medical research, or law-enforcement investigations or with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the genetic information will be collected, processed, or transferred with such a notice provided for each instance in which such collection, processing, or transferring is to occur. **[**(7) The transfer of an individual's aggregated internet search or browsing history, except with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the individual's aggregated internet search or browsing history will be transferred with such a notice provided for each instance in which such transfer is to occur or a search warrant or exigent circumstances.**]** (8) The transfer of an individual's physical activity information from a smart phone or wearable device, other than to another device or service of that individual with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the physical activity information will be transferred with such a notice provided for each instance in which such transfer is to occur absent a search warrant or exigent circumstances.
Notes: Applies to Everyone.	

Not included in Cantwell. Prohibits collection, transfer, and processing of certain sensitive information, such as SSN, geolocation, biometric, password, nonconsensual nudity, and genetic information.

Cantwell	**Three Corners**
--	SEC. 103. PRIVACY BY DESIGN. (a) POLICIES, PRACTICES, AND PROCEDURES. —A covered entity shall establish and implement reasonable policies, practices, and procedures regarding the collection, processing, and transfer of covered data to— (1) consider Federal, State, or local laws, rules, or regulations related to covered data the covered entity collects, processes, or transfers; (2) consider the mitigation of privacy risks related to individuals under the age of 17; (3) consider the mitigation of privacy risks related to the products and services of the covered entity, including their design, development, and implementation; and (4) implement reasonable training and safeguards within the covered entity to promote compliance with all privacy laws applicable to covered data the covered entity collects, processes, or transfers and mitigate privacy risks. (b) FACTORS TO CONSIDER. —The policies, practices, and procedures established by a covered entity under subsection (a), shall correspond with— (1) the size of the covered entity and the nature, scope, and complexity of the activities engaged in by the covered entity; (2) the sensitivity of the covered data collected, processed, or transferred by the covered entity; (3) the volume of covered data collected, processed, or transferred by the covered entity; (4) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates; and (5) the cost of implementing the program in relation to the risks and nature of the covered data. (c) COMMISSION GUIDANCE. —Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance as to what constitutes reasonable policies, practices, and procedures as required by this section.
Notes: Applies to Covered Entities.	

Not included in Cantwell. Must establish policies and procedures to comply with relevant laws, mitigate privacy risks to individuals under 17, and implement employee training. FTC to provide guidance.

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 207. PROHIBITION ON DENIAL OF SERVICE AND WAIVER OF RIGHTS. (a) Conditional Service or Pricing Prohibited. —A covered entity shall not deny, charge different prices or rates, or condition the provision of a service or product to an individual on the individual's agreement to waive privacy rights guaranteed by— (1) sections 101, 102, 201, 202(a)(1), 202(a)(2), 202(a)(4), 204, and 205; or (2) sections 202(a)(3), 203(a), and 203(c), except in the case where— (A) there exists a direct relationship between the individual and the covered entity that is initiated by the individual; (B) the provision of the service or product requested by the individual requires the processing or transferring of the covered data of the individual and the covered data is [strictly] necessary to provide the service or product; and (C) the individual provides affirmative express consent to such processing or transfer. (b) Rule of Application. —In addition to the original product or service offered to consumers in compliance with subsection (a)(2), a covered entity may offer different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a right described in subsection (a)(2).	**SEC. 207. PROHIBITION ON DENIAL OF SERVICE AND WAIVER OF RIGHTS.** (a) CONDITIONAL SERVICE OR PRICING PROHIBITED. —A covered entity shall not deny, charge different prices or rates, or condition the provision of a service or product to an individual on the individual's agreement to waive privacy rights guaranteed by— (1) sections 101, 102, 201, 202(a)(1), 202(a)(2), 202(a)(4), 204, and 205; or (2) sections 202(a)(3), 203(a), and 203(c), except in the case where— (A) there exists a direct relationship between the individual and the covered entity that is initiated by the individual; (B) the provision of the service or product requested by the individual requires the processing or transferring of the covered data of the individual and the covered data is strictly necessary to provide the service or product; and (C) the individual provides affirmative express consent to such processing or transfer. (b) RULE OF APPLICATION. —In addition to the original product or service offered to consumers in compliance with subsection (a)(2), a covered entity may offer different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a right described in subsection (a)(2).	SEC. 104. LOYALTY TO INDIVIDUALS WITH RESPECT TO PRICING. (a) CONDITIONAL SERVICE OR PRICING PROHIBITED.—A covered entity shall not deny, charge different prices or rates, or condition **or effectively condition** the provision of a service or product to an individual on the individual's agreement to waive any privacy rights **guaranteed by this Act or any regulations promulgated under this Act or terminate a service or otherwise refuse to provide a service or product to an individual as a consequence of the individual's refusal to waive any such privacy rights.** (b) RULES OF CONSTRUCTION. —Nothing in subsection (a) shall be construed to prohibit— (1) the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and used only for the purpose of initiating, rendering, billing for, or collecting payment for a service or product requested by the individual; or

		(2) a covered entity from offering a loyalty program that provides discounted or free products or services, or other consideration, in exchange for an individual's continued business with the covered entity, provided that such program otherwise complies with the requirements of this Act and any regulations promulgated under this Act.
Notes: Applies to Covered Entities. Cantwell prohibits price discrimination or refusal to offer services based on exercise of rights. Sec. (a)(2) appears to grandfather in existing consent to data practices. Three Corners does not appear to grandfather existing consent and clarifies Cantwell intent that the pricing discrimination does not prohibit loyalty programs or discounts.		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 201. TRANSPARENCY. (a) In General. —Each covered entity shall make publicly available, in a clear, conspicuous, and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the entity's data processing and data transfer activities. (b) Content of Privacy Policy. —The privacy policy required under subsection (a) shall include, at a minimum, the following: (1) The identity and the contact information of— (A) the covered entity (including the covered entity's points of contact for privacy and data security inquiries); and (B) any affiliate to which covered data may be transferred by the covered entity.	SEC. 201. TRANSPARENCY. (a) IN GENERAL. —Each covered entity shall make publicly available, in a clear, conspicuous, and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the entity's data processing and data transfer activities. (b) CONTENT OF PRIVACY POLICY. —The privacy policy required under subsection (a) shall include, at a minimum, the following: (1) The identity and the contact information of— (A) the covered entity (including the covered entity's points of contact for privacy and data security inquiries); and (B) any affiliate to which covered data may be transferred by the covered entity.	SEC. 202. TRANSPARENCY. (a) IN GENERAL. —Each covered entity shall make publicly available, in a clear, conspicuous, and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the entity's data collection, processing, and transfer activities. (b) CONTENT OF PRIVACY POLICY. —The privacy policy required under subsection (a) shall include, at a minimum, the following: (1) The identity and the contact information of— (A) the covered entity (including the covered entity's points of contact, **generic electronic mail addresses, and phone numbers of the covered entity, as applicable** for privacy and data security inquiries); and (B) any other entity **within the same corporate structure as the covered entity** to which covered data has been or may be transferred by the covered entity.

(2) The categories of covered data the covered entity collects. (3) The processing purposes for each category of covered data the covered entity collects. (4) Whether the covered entity transfers covered data and, if so, each category of service provider and third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such categories, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such transfer.	(2) The categories of covered data the covered entity collects. (3) The processing purposes for each category of covered data the covered entity collects. (4) Whether the covered entity transfers covered data and, if so, each category of service provider and third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such categories, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such transfer.	(2) The categories of covered data the covered entity collects or processes. (3) The processing purposes for each category of covered data the covered entity collects or processes. (4) Whether the covered entity transfers covered data and, if so, each category of service provider and third party to which the covered entity transfers covered data, **the name of each third-party collecting entity to which the covered entity transfers covered data**, and the purposes for which such data is transferred to such categories **of service providers and third parties or third-party collecting entities**, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such transfer.
(5) The length of time the covered entity intends to retain each category of covered data, including sensitive covered data, or, if it is not possible to identify that time frame, the criteria used to determine the length of time the covered entity intends to retain categories of covered data. (6) How an individual can exercise the rights described in this title. (7) A general description of the covered entity's data security practices. (8) The effective date of the privacy policy.	(5) The length of time the covered entity in14 tends to retain each category of covered data, including sensitive covered data, or, if it is not possible to identify that time frame, the criteria used to determine the length of time the covered entity intends to retain categories of covered data. (6) How an individual can exercise the rights described in this title. (7) A general description of the covered entity's data security practices. (8) The effective date of the privacy policy.	(5) The length of time the covered entity intends to retain each category of covered data, including sensitive covered data, or, if it is not possible to identify that time frame, the criteria used to determine the length of time the covered entity intends to retain categories of covered data. (6) How an individual can exercise the rights described in this title. (7) A general description of the covered entity's data security practices. (8) The effective date of the privacy policy. **(9) Whether or not any covered data collected by the covered entity is transferred to, processed in, or otherwise made available to the People's Republic of China, Russia, Iran, or North Korea.**
C) Languages. —The privacy policy required under subsection (a) shall be made available to the public in each language in which the covered entity—	(C) LANGUAGES. —The privacy policy required under subsection (a) shall be made available to the public in each language in which the covered entity—	C) LANGUAGES. —The privacy policy required under subsection (a) shall be made available to the public in each language in which the covered entity—

(1) provides a product or service that is subject to the privacy policy; or (2) carries out activities related to such products or services.	(1) provides a product or service that is subject to the privacy policy; or (2) carries out activities related to such product or service.	(1) provides a product or service that is subject to the privacy policy; or (2) carries out activities related to such products or services.
(d) Material Changes. —	(d) MATERIAL CHANGES. —	(d) MATERIAL CHANGES. —
(1) AFFIRMATIVE EXPRESS CONSENT. —A covered entity shall not make a material change to its privacy policy or practices ~~with respect to previously collected covered data~~ without first obtaining affirmative express consent from each affected individual.	(1) AFFIRMATIVE EXPRESS CONSENT. — A covered entity shall not make a material change to its privacy policy or practices with respect to previously collected covered data without first obtaining affirmative express consent from each affected individual.	(1) AFFIRMATIVE EXPRESS CONSENT.—If a covered entity makes a material change to its privacy policy or practices, **the covered entity shall notify each individual affected by such material change before further processing or transferring any previously collected covered data and, except as provided in paragraphs (3) and (4) of section 209(a), provide a reasonable opportunity for each individual to withdraw consent to any further collecting, processing or transferring of covered data under the changed policy.**
(2) NOTIFICATION. —The covered entity shall provide direct notification, where possible, regarding material changes to the privacy policy to each affected individual, taking into account available technology and the nature of the relationship.	(2) NOTIFICATION. —The covered entity shall provide direct notification, where possible, regarding material changes to the privacy policy to each affected individual, taking into account available technology and the nature of the relationship.	(2) NOTIFICATION. —The covered entity shall take all reasonable measures to provide direct notification regarding material changes to the privacy policy to each affected individual, in each language that the privacy policy is made, and taking into account available technology and the nature of the relationship. **(3) CLARIFICATION. —Nothing in this section shall be construed to affect the requirements for covered entities under section 204.**
(e) Short form Notice to Consumers by Large Data Holders. —	(e) SHORT-FORM NOTICE TO CONSUMERS BY LARGE DATA HOLDERS. —	(e) SHORT-FORM NOTICE TO CONSUMERS BY LARGE DATA HOLDERS. —
(1) IN GENERAL. —In addition to the privacy policy required under subsection (a), a large data holder must provide a short-form notice of its covered data practices in a manner that is—	(1) IN GENERAL. —In addition to the privacy policy required under subsection (a), a large data holder must provide a short-form notice of its covered data practices in a manner that is—	(1) IN GENERAL. —In addition to the privacy policy required under subsection (a), a large data holder must provide a short-form notice of its covered data practices in a manner that is—
(A) concise, clear, and conspicuous;	(A) concise, clear, and conspicuous;	(A) concise, clear, and conspicuous;

(B) readily accessible, based on the way an individual interacts with the large data holder and its products or services and what is reasonably anticipated within the context of the relationship; and (C) inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may be unexpected or that involve sensitive covered data. (2) RULEMAKING. —The Commission shall issue a rule pursuant to section 553 of title 5, United States Code, establishing the minimum data disclosures necessary for the short-form notice based solely on the content requirements in subsection (b).	(B) readily accessible, based on the way an individual interacts with the large data holder and its products or services and what is reasonably anticipated within the context of the relationship; and (C) inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may be unexpected or that involve sensitive covered data. (2) RULEMAKING. —The Commission shall issue a rule pursuant to section 553 of title 5, United States Code, establishing the minimum data disclosures necessary for the short-form notice based solely on the content requirements in subsection (b).	(B) readily accessible, based on the way an individual interacts with the large data holder and its products or services and what is reasonably anticipated within the context of the relationship; and (C) inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected or that involve sensitive covered data. (2) RULEMAKING. —The Commission shall issue a rule pursuant to section 553 of title 5, United States Code, establishing the minimum data disclosures necessary for the short-form notice based solely on the content requirements in subsection (b).
Notes: Applies to Covered Entities, Large Data Holders, FTC. Requires published, multilingual privacy policy and contact information for privacy concerns. Prohibits changing material terms (in Cantwell, only for previously collected data) without notifying consumers. Large Data Holders must provide additional, short form notice of privacy policies and data rights. FTC to conduct rulemaking to promulgate minimum disclosure standards for Large Data Providers.		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 202. INDIVIDUAL CONTROL. (a) Access to, and Correction, Deletion, and Portability of, Covered Data. —Subject to subsections (b) and (c), a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to— (1) access— (A) the covered data of the individual~~, or an accurate representation of the covered data of the individual~~ in a human-readable format that a reasonable individual can understand,	SEC. 202. INDIVIDUAL CONTROL. (a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF COVERED DATA. —Subject to subsections (b) and (c), a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to— (1) access— (A) the covered data of the individual, or an accurate representation of the covered data of the individual in a human-readable format that a reasonable individual can understand,	SEC. 203. INDIVIDUAL DATA OWNERSHIP AND CONTROL. (a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA. —Subject to subsections (b) and (c), a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to— (1) access— (A) the covered data of the individual in a human-readable format that a reasonable individual can understand and download from the Internet, that is **collected**, processed or transferred by

that is processed or transferred by the covered entity ~~and~~ any service provider of the covered entity; (B) the name of any third party or service provider to whom the covered entity has transferred the covered data of the individual, as well as the categories of sources from which the covered data was collected; ~~and~~ (C) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;	that is processed or transferred by the covered entity and any service provider of the covered entity; (B) the name of any third party or service provider to whom the covered entity has transferred the covered data of the individual, as well as the categories of sources from which the covered data was collected; and (C) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;	the covered entity **or** any service provider of the covered entity; (B) the name of any third party**, other covered entity**, or service provider to whom the covered entity has transferred the covered data of the individual, as well as the categories of sources from which the covered data was collected; (C) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party, **other covered entity,** or service provider; **and** **(D) with respect to covered data that is no longer in the possession of the covered entity, a general description, in a human-readable format that a reasonable individual can understand, of the covered data that the covered entity collected, processed, or transferred;**
(2) correct any inaccuracy or incomplete information with respect to the covered data of the individual that is processed by the covered entity and notify any third party or service provider to which the covered entity transferred such covered data of the corrected information; (3) delete covered data of the individual that is processed by the covered entity and request that the covered entity notify any third party or service provider to which the covered entity transferred such covered data of the individual's deletion request; and (4) to the extent technically feasible, export covered data, except for derived data, of the individual that is processed by the covered entity without licensing restrictions that limit such transfers, in— (A) a human-readable format that a reasonable individual can understand; and	(2) correct any inaccuracy or incomplete information with respect to the covered data of the individual that is processed by the covered entity and notify any third party or service provider to which the covered entity transferred such covered data of the corrected information; (3) delete covered data of the individual that is processed by the covered entity and request that the covered entity notify any third party or service provider to which the covered entity transferred such covered data of the individual's deletion request; and (4) to the extent technically feasible, export covered data, except for derived data, of the individual that is processed by the covered entity without licensing restrictions that limit such transfers, in— (A) a human-readable format that a reasonable individual can understand; and	(2) correct any inaccuracy or incomplete information with respect to the covered data of the individual that is processed by the covered entity and notify any third party, **other covered entity,** or service provider to which the covered entity transferred such covered data of the corrected information; (3) delete covered data of the individual that is processed by the covered entity and notify any third party, **other covered entity,** or service provider to which the covered entity transferred such covered data of the individual's deletion request; and (4) to the extent technically feasible, export covered data, except for derived data, of the individual that is processed by the covered entity without licensing restrictions that limit such transfers, in— (A) a human-readable format that a reasonable individual can understand **and download from the Internet**; and

(B) a portable, structured, interoperable, and machine-readable format.	(B) a portable, structured, interoperable, and machine-readable format.	(B) a portable, structured, interoperable, and machine-readable format. **(b) TIMING. — Subject to subsections (c) and (d) each request shall be completed by any—** **(1) large data holder within [30 days] of verification of such request from an individual;** **(2) covered entity that is not considered a large data holder or a covered entity described in 209(c) within [60 days] of verification of such request from an individual;** **(3) covered entity as described in 209(c) within [90 days] of verification of such request from an individual.**
(b) Frequency and Cost of Access. —A covered entity— (1) shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and (2) with respect to— (A) the first 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and (B) any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a reasonable fee for each request.	(b) FREQUENCY AND COST OF ACCESS. —A covered entity— (1) shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and (2) with respect to— (A) the first 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and (B) any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a reasonable fee for each request.	(c) FREQUENCY AND COST OF ACCESS. —A covered entity— (1) shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and (2) with respect to— (A) the first 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and (B) any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a reasonable fee for each request.
(c) Verification and Exceptions. — (1) REQUIRED EXCEPTIONS. —A covered entity shall not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity— (A) cannot reasonably verify that the individual making the request to exercise the right is the individual	(c) VERIFICATION AND EXCEPTIONS. — (1) REQUIRED EXCEPTIONS. —A covered entity shall not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity— (A) cannot reasonably verify that the individual making the request to exercise the right is the individual	(d) VERIFICATION AND EXCEPTIONS. — (1) REQUIRED EXCEPTIONS. —A covered entity shall not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity— (A) cannot reasonably verify that the individual making the request to exercise the right is the individual

whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf; or (B) reasonably believes that the request is made to interfere with a contract between the covered entity and another individual. (2) ADDITIONAL INFORMATION. —If a covered entity cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity— (A) shall request that the individual making the request to exercise the right provide any additional information necessary for the sole purpose of verifying the identity of the individual; and (B) shall not process or transfer such additional information for any other purpose. (3) PERMISSIVE EXCEPTIONS. — (A) IN GENERAL. —A covered entity may decline to comply with a request to exercise a right described in subsection (a), in whole or in part, that would— (i) require the entity to retain any covered data collected for a single, one-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction. (ii) be impossible or demonstrably impracticable to comply with.	whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf; or (B) reasonably believes that the request is made to interfere with a contract between the covered entity and another individual. (2) ADDITIONAL INFORMATION. —If a covered entity cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity— (A) shall request that the individual making the request to exercise the right provide any additional information necessary for the sole purpose of verifying the identity of the individual; and (B) shall not process or transfer such additional information for any other purpose. (3) PERMISSIVE EXCEPTIONS. — (A) IN GENERAL. —A covered entity may decline to comply with a request to exercise a right described in subsection (a), in whole or in part, that would— (i) require the entity to retain any covered data collected for a single, one time transaction if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction; (ii) be impossible or demonstrably impracticable to comply with;	whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf; or (B) reasonably believes that the request is made to interfere with a contract between the covered entity and another individual. (2) ADDITIONAL INFORMATION. —If a covered entity cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity— (A) shall request that the individual making the request to exercise the right provide any additional information necessary for the sole purpose of verifying the identity of the individual; and (B) shall not process or transfer such additional information for any other purpose. (3) PERMISSIVE EXCEPTIONS. — (A) IN GENERAL. —A covered entity may decline to comply with a request to exercise a right described in subsection (a), in whole or in part, that would— (i) require the **covered** entity to retain any covered data collected for a single, one-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction. (ii) be impossible or demonstrably impracticable to comply with**, and the covered entity shall provide a description to the requestor detailing the inability to comply with the request**.

(iii) require the covered entity to re-identify covered data that is de-identified data. (iv) result in the release of trade secrets, or other proprietary or confidential data or business practices.	(iii) require the covered entity to re-identify covered data that is de-identified data; (iv) result in the release of trade secrets, or other proprietary or confidential data or business practices;	(iii) require the covered entity to re-identify covered data that is de-identified data; (iv) result in the release of trade secrets, or other proprietary or confidential data or business practices. **(v) require the covered entity to correct any covered data that cannot be reasonably verified as being inaccurate or incomplete.**
(v) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, or investigate malicious or unlawful activity, or enforce contracts; or (vi) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States.	(v) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, or investigate malicious or unlawful activity, or enforce contracts; or (vi) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States.	(vi) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, or investigate malicious or unlawful activity, or enforce valid contracts; or (vii) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States.
(B) NUMBER OF REQUESTS. —For purposes of this paragraph, the receipt of a large number of verified requests, on its own, shall not be considered to render compliance with a request demonstrably impossible.	(B) NUMBER OF REQUESTS. —For purposes of this paragraph, the receipt of a large number of verified requests, on its own, shall not be considered to render compliance with a request demonstrably impossible.	(B) NUMBER OF REQUESTS. —For purposes of this paragraph, the receipt of many verified requests, on its own, shall not be considered to render compliance with a request demonstrably impossible.
(d) Regulations. —The Commission is authorized to enact interpretive rules pursuant to section 553 of title 5, United States Code (5 U.S.C. 553), ~~to clarify or explain the provisions of this section and establish processes by which a covered entity may verify a request to exercise a right described in subsection (a).~~	(d) REGULATIONS. —The Commission is authorized to enact interpretive rules pursuant to section 553 of title 5, United States Code (5 U.S.C. 553), to clarify or explain the provisions of this section and establish processes by which a covered entity may verify a request to exercise a right described in subsection (a).	(d) REGULATIONS. —The Commission is authorized to enact regulations pursuant to section 553 of title 5, United States Code (5 U.S.C. 553), **as necessary to establish processes by which covered entities are to comply with the provisions of this section. Such regulations shall take into consideration—** **(1) the size of, and the nature, scope, and complexity of the activities engaged in by the covered entity, including whether the covered entity is a large data holder or third-party collecting entity.** **(2) the sensitivity of covered data collected, processed, or transferred by the covered entity.** **(3) the volume of covered data collected, processed, or transferred by the covered entity; and**

		(4) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates.
Notes: Applies to Covered Entities, Large Data Holders, Service Providers, FTC. Allows individuals to request access, correct, delete, or export their covered data. Covered Entities are required to not process requests where the Covered Entity cannot verify the identity of the individual or has reason to believe the request is spurious. Covered Entities may decline to process requests that they believe require retaining data longer than possible, may be impossible or impractical, interfere with law enforcement, violate law, reveal trade secrets, or (Three Corners Only) require companies to correct data that is not demonstrably false. Requires the FTC to conduct rulemaking on compliance. Three Corners provides additional specificity for the rulemaking.		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 203. RIGHT TO CONSENT AND OBJECT. (a) Sensitive Covered Data Consent Requirements. —Without the affirmative express consent of an individual, a covered entity shall not process the sensitive covered data of the individual or transfer such sensitive covered data to a third party. (b) Withdrawal of Consent. —A covered entity shall provide an individual with a clear and conspicuous means to withdraw affirmative express consent previously provided by the individual with respect to the processing or transfer of the covered data of the individual. (c) Right to Opt Out of Covered Data Transfers. — (1) IN GENERAL. —A covered entity— (A) shall not transfer the covered data of an individual to a third party if the individual objects to the transfer; and	SEC. 203. RIGHT TO CONSENT AND OBJECT. (a) SENSITIVE COVERED DATA CONSENT REQUIREMENTS. —Without the affirmative express consent of an individual, a covered entity shall not process the sensitive covered data of the individual or transfer such sensitive covered data to a third party. (b) WITHDRAWAL OF CONSENT. —A covered entity shall provide an individual with a clear and conspicuous means to withdraw affirmative express consent previously provided by the individual with respect to the processing or transfer of the covered data of the individual. (c) RIGHT TO OPT OUT OF COVERED DATA TRANSFERS. — (1) IN GENERAL. —A covered entity— (A) shall not transfer the covered data of an individual to a third party if the individual objects to the transfer; and	SEC. 204. RIGHT TO CONSENT AND OBJECT. (a) SENSITIVE COVERED DATA CONSENT REQUIREMENTS. —Without the affirmative express consent of an individual, a covered entity shall not collect or process the sensitive covered data of the individual or transfer such sensitive covered data to a third party. (b) WITHDRAWAL OF CONSENT. —A covered entity shall provide an individual with a clear and conspicuous, **easy-to-execute** means to withdraw **any** affirmative express consent previously provided by the individual **that are as easy to execute by a reasonable individual as the means to provide consent,** with respect to the processing or transfer of the covered data of the individual. (c) RIGHT TO OPT OUT OF COVERED DATA TRANSFERS. — (1) IN GENERAL. —A covered entity— (A) shall not transfer the covered data of an individual to a third party if the individual objects to the transfer; and

(B) shall allow an individual to object to such transfer through an opt-out mechanism, as described in paragraph (2). ~~(2) FEASIBILITY STUDY AND RULEMAKING. —~~ ~~(A) FEASIBILITY STUDY. —Not later than 1 year after the date of enactment of this Act, the Commission shall initiate and finalize a feasibility study on the creation of a privacy protective, centralized opt-out mechanism to minimize the number of opt-out designations of a similar type that an individual must make.~~ ~~(B) RULEMAKING. —If the Commission determines that a centralized opt-out mechanism is feasible under subparagraph (A), the Commission shall issue a rule under section 553 of title 5, United States Code, establishing 1 or more acceptable opt-out mechanisms for a covered entity to utilize to allow an individual to opt out of the transfer of covered data related to such individual.~~ (d) Right to Opt Out of Targeted Advertising. ~~—A large data holder~~ that engages in targeted advertising shall— (1) provide an individual with a clear and conspicuous means to opt out of targeted advertising; and (2) abide by such opt-out designations by an individual.	(B) shall allow an individual to object to such transfer through an opt-out mechanism, as described in paragraph (2). (2) FEASIBILITY STUDY AND RULEMAKING. — (A) FEASIBILITY STUDY. —Not later than 1 year after the date of enactment of this Act, the Commission shall initiate and finalize a feasibility study on the creation of a privacy protective, centralized opt-out mechanism to minimize the number of opt-out designations of a similar type that an individual must make. (B) RULEMAKING. —If the Commission determines that a centralized opt-out mechanism is feasible under subparagraph (A), the Commission shall issue a rule under section 553 of title 5, United States Code, establishing 1 or more acceptable opt-out mechanisms for a covered entity to utilize to allow an individual to opt out of the transfer of covered data related to such individual. (d) RIGHT TO OPT OUT OF TARGETED ADVERTISING. —A large data holder that engages in targeted advertising shall— (1) provide an individual with a clear and conspicuous means to opt out of targeted advertising; and (2) abide by such opt-out designations by an individual.	(B) shall allow an individual to object to such transfer through an opt-out mechanism, as described in section 210(b), **if applicable.** (d) RIGHT TO OPT OUT OF TARGETED ADVERTISING. —**A covered entity that engages in targeted advertising shall—** (1) **prior to engaging in such targeted advertising and at all times, thereafter**, provide an individual with a clear and conspicuous means to opt out of targeted advertising; (2) abide by such opt-out designations by an individual; **and** **(3) shall allow an individual to prohibit such targeted advertising through an opt-out mechanism, as described in section 210(b), if applicable.**
Notes: Applies to Covered Entities, Large Data Holders, FTC		

Prohibits the transfer of Sensitive Covered Data without affirmative consumer consent. Places standards for obtaining consent, including that it must be a clear, understandable mechanism. Three Corners requires mechanism for withdrawing consent to be as simple as that for obtaining consent.

Cantwell would direct FTC to conduct rulemaking to determine feasibility and implement centralized acceptable opt-out mechanism. Three Corners establishes this rulemaking in its Section 204.

Both allow consumers to opt out of targeted advertising, though Cantwell would only allow opt-out from advertising conducted by a Large Data Holder. Three Corners provides opt-out for all.

Cantwell	**Three Corners**
--	SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MINORS. (a) PROHIBITION ON TARGETED ADVERTISING TO CHILDREN AND MINORS. —A covered entity shall not engage in targeted advertising to any individual under the age of 17 if the covered entity has [actual knowledge] that the individual is under the age of 17. (b) DATA TRANSFER REQUIREMENTS RELATED TO MINORS. —A covered entity shall not transfer the covered data of an individual to a third party without affirmative express consent from the individual or the individual's parent or guardian if the covered entity [has actual knowledge] that the individual is between 13 and 17 years of age. (c) YOUTH PRIVACY AND MARKETING DIVISION. — (1) ESTABLISHMENT. —There is established within the Commission a division to be known as the "Youth Privacy and Marketing Division" (in this section referred to as the "Division"). (2) DIRECTOR. —The Division shall be headed by a Director, who shall be appointed by the Chair of the Commission. (3) DUTIES. —The Division shall be responsible for addressing, as it relates to this Act— (A) the privacy of children and minors; and (B) marketing directed at children and minors. (4) STAFF. —The Director of the Division shall hire adequate staff to carry out the duties described in paragraph (3), including by hiring individuals who are experts in data protection, digital advertising, data analytics, and youth development. (5) REPORTS. —Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Commission shall submit to the Committee on Commerce,

	Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that includes— (A) a description of the work of the Division regarding emerging concerns relating to youth privacy and marketing practices; and (B) an assessment of how effectively the Division has, during the period for which the report is submitted, addressed youth privacy and marketing practices. (d) REPORT BY THE INSPECTOR GENERAL. — (1) IN GENERAL. —Not later than 2 years after the date of enactment of this Act, and biennially thereafter, the Inspector General of the Commission shall submit to the Commission and to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report regarding the safe harbor provisions in section 1307 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6503), which shall include— (A) an analysis of whether the safe harbor provisions are— (i) operating fairly and effectively; and (ii) effectively protecting the interests of children and minors; and (B) any proposal or recommendation for policy changes that would improve the effectiveness of the safe harbor provisions. (2) PUBLICATION. —Not later than 10 days after the date on which a report is submitted under paragraph (1), the Commission shall publish the report on the website of the Commission.
Notes: Applies to Covered Entities, FTC. Not included in Cantwell. Prohibits targeted advertising to individuals who a Covered Entity has actual knowledge are under 17. Prohibits data transfers of individuals who a Covered Entity has actual knowledge are between 13 and 17 without Express Affirmative Consent. Establishes new Bureau in the FTC to enforce privacy and advertising provisions related to children.	

Cantwell	**Three Corners**
--	SEC. 206. THIRD-PARTY COLLECTING ENTITIES.

	(a) NOTICE. —Each third-party collecting entity shall place a clear and conspicuous notice on the website or mobile application of the third-party collecting entity (if the third-party collecting entity maintains such a website or mobile application) that— (1) notifies individuals that the entity is a third-party collecting entity using specific language that the Commission shall develop through rulemaking under section 553 of title 5, United States Code; and (2) includes a link to the website established under subsection(c)(3). (b) REQUIRED AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION. —Not later than [1 year] after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code to require third-party collecting entities to establish measures that allow for and facilitate the auditing by an individual of any internal or external access to, or disclosure of, any covered data relating to such individual processed by such third-party collecting entity. (c) THIRD-PARTY COLLECTING ENTITY REGISTRATION. — (1) IN GENERAL. — Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a third-party collecting entity [and processed covered data pertaining to more than [5,000] individuals or devices that identify or are linked or reasonably linkable to an individual] shall register with the Commission in accordance with this subsection. (2) REGISTRATION REQUIREMENTS. —In registering with the Commission as required under paragraph (1), a third-party collecting entity shall do the following: (A) Pay to the Commission a registration fee of $100. (B) Provide the Commission with the following information: (i) The legal name and primary physical, email, and internet addresses of the third-party collecting entity. (ii) a description of the categories of data the third-party collecting entity processes and transfers. (iii) the contact information of the third-party collecting entity, including a contact person, telephone number, an e-mail address, a website, and a physical mailing address; and (iv) link to a website through which an individual may easily exercise the rights provided under subsection (b) of this section.

	(3) THIRD-PARTY COLLECTING ENTITY REGISTRY. —The Commission shall establish and maintain on a website a searchable, publicly available, central registry of third-party collecting entities that are registered with the Commission under this subsection that includes the following: (A) A listing of all third-party collecting entities and a search feature that allows members of the public to identify individual third-party collecting entities. (B) For each registered third-party collecting entity, the information described in paragraph (2). (C) Links to individual third-party collecting entities through which an individual may easily exercise the rights provided under subsection (b) of this section. (D) A "Do Not Collect" registry link and mechanism by which an individual may, after the Commission has verified the identity of the individual or individual's parent or guardian, which may include tokenization, easily submit a request to all registered third-party collecting entities that are not consumer reporting agencies as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) to (i) delete all covered data related to such individual that the third-party collecting entity did not collect from the individual directly or when acting as a service provider; and (ii) ensure that any third-party collecting entity no longer collects covered data related to such individual without the affirmative express consent of such individual, except insofar as such covered entity is acting as a service provider. Each third-party collecting entity that receives such a request from an individual shall delete all the covered data of the individual not later than [30 days] after the request is received by the third-party collecting entity. (d) PENALTIES. —A third-party collecting entity that fails to register or provide the notice as required under this section shall be liable for— (1) a civil penalty of $50 for each day it fails to register or provide notice as required under this subsection, not to exceed a total of $10,000 for any year; and (2) an amount equal to the registration fees due under paragraph (2) of subsection (c) for each year that it failed to register as required under paragraph (1) of such subsection.
Notes: Applies to Third-Party Collecting Entities, FTC Not included in Cantwell.	

FTC directed to establish a published third-party collector registry listing all Third-Party Collecting Entities with contact information and description of their data process. FTC creates a "Do Not Collect" link that allows individuals to opt-out of collection and request data deletion from all registered Entities.

Third-Party Collecting Entities must pay to register and face fines up to $10,000 annually for failure to register.

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 204. CIVIL RIGHTS AND ALGORITHMS.	SEC. 204. CIVIL RIGHTS AND ALGORITHMS.	SEC. 207. CIVIL RIGHTS AND ALGORITHMS.
(a) Civil Rights Protections. —	(a) CIVIL RIGHTS PROTECTIONS. —	(a) CIVIL RIGHTS PROTECTIONS. —
(1) IN GENERAL. —A covered entity may not process covered data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, gender, sexual orientation, or disability.	(1) IN GENERAL. —A covered entity may not process covered data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, gender, sexual orientation, or disability.	(1) IN GENERAL. —A covered entity may not **collect**, process, or transfer covered data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, gender, sexual orientation, or disability.
(2) EXCEPTIONS. —This subsection shall not apply to—	(2) EXCEPTIONS. —This subsection shall not apply to—	(2) EXCEPTIONS. —This subsection shall not apply to—
(A) the processing of covered data for the purpose of—	(A) the processing of covered data for the purpose of—	(A) the **collection**, processing, **or transfer** of covered data for the purpose of—
(i) a covered entity's self-testing to prevent discrimination; or	(i) a covered entity's self-testing to prevent discrimination; or	(i) a covered entity's self-testing to prevent discrimination; or
(ii) **expanding an** applicant, participant, or customer pool **by increasing diversity and inclusion**; or	(ii) expanding an applicant, participant, or customer pool by increasing diversity and inclusion; or	(ii) diversifying an applicant, participant, or customer pool; or
(B) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).	(B) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).	(B) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).
(b) FTC Enforcement Assistance. —	(b) FTC ENFORCEMENT ASSISTANCE. —	(b) FTC ENFORCEMENT ASSISTANCE. —
(1) IN GENERAL. —Whenever the Commission obtains information that a covered entity may have processed or transferred covered data in violation of subsection (a), the Commission shall transmit such information as allowable	(1) IN GENERAL. —Whenever the Commission obtains information that a covered entity may have processed or transferred covered data in violation of subsection (a), the Commission shall	(1) IN GENERAL. —Whenever the Commission obtains information that a covered entity may have **collected**, processed, or transferred covered data in violation of subsection (a), the Commission shall transmit such

under Federal law to any Executive agency with authority to initiate proceedings relating to such violation.	transmit such information as allowable under Federal law to any Executive agency with authority to initiate proceedings relating to such violation.	information as allowable under Federal law to any Executive agency with authority to initiate proceedings relating to such violation.
(2) ANNUAL REPORT. —Not later than [SLC Note: To be provided] months after the date of enactment of this Act, and annually thereafter, the Commission shall submit to Congress a report that includes a summary of—	(2) ANNUAL REPORT. —Not later than [*SLC Note: To be provided]* months after the date of enactment of this Act, and annually thereafter, the Commission shall submit to Congress a report that includes a summary of—	(2) ANNUAL REPORT. —Not later than [___] months after the date of enactment of this Act, and annually thereafter, the Commission shall submit to Congress a report that includes a summary of—
(A) the types of information the Commission transmitted to Federal agencies under paragraph (1) during the previous 1-year period; and (B) how such information relates to Federal civil rights laws.	(A) the types of information the Commission transmitted to Federal agencies under paragraph (1) during the previous 1-year period; and (B) how such information relates to Federal civil rights laws.	(A) the types of information the Commission transmitted to Federal agencies under paragraph (1) during the previous 1-year period; and (B) how such information relates to Federal civil rights laws.
(3) TECHNICAL ASSISTANCE. —In transmitting information under paragraph (1), the Commission may consult and coordinate with, and provide technical and investigative assistance to, such Executive agency.	(3) TECHNICAL ASSISTANCE. —In transmitting information under paragraph (1), the Commission may consult and coordinate with, and provide technical and investigative assistance to, such Executive agency.	(3) TECHNICAL ASSISTANCE. —In transmitting information under paragraph (1), the Commission may consult and coordinate with, and provide technical and investigative assistance to, such Executive agency.
(4) COOPERATION WITH OTHER AGENCIES. —The Commission may implement this subsection by executing agreements or memoranda of understanding with the appropriate Federal agencies.	(4) COOPERATION WITH OTHER AGENCIES. — The Commission may implement this subsection by executing agreements or memoranda of understanding with the appropriate Federal agencies.	(4) COOPERATION WITH OTHER AGENCIES. —The Commission may implement this subsection by executing agreements or memoranda of understanding with the appropriate Federal agencies.
(5) OFFICE OF CIVIL RIGHTS ESTABLISHMENT. —	(5) OFFICE OF CIVIL RIGHTS ESTABLISHMENT. —	
(A) IN GENERAL. —Not later than 1 year after the date of enactment of this Act, the Commission shall establish an Office of Civil Rights, which shall assist the Commission in exercising its authority under this section. **(B) STAFF AND RESOURCES. —The Commission shall provide the Office of Civil Rights such staff and resources as are necessary to carry out this section.**	(A) IN GENERAL. —Not later than 1 year after the date of enactment of this Act, the Commission shall establish an Office of Civil Rights, which shall assist the Commission in exercising its authority under this section. (B) STAFF AND RESOURCES. — The Commission shall provide the Office of Civil Rights such staff and resources as are necessary to carry out this section.	

(c) Algorithm Impact and Evaluation. —	(c) ALGORITHM IMPACT AND EVALUATION. —	(c) ALGORITHM IMPACT AND EVALUATION. —
(1) ALGORITHM IMPACT ASSESSMENT. —	(1) ALGORITHM IMPACT ASSESSMENT. —	(1) ALGORITHM IMPACT ASSESSMENT. —
(A) IMPACT ASSESSMENT. — Notwithstanding any other provision of law, not later than [SLC Note: To be provided] after the date of enactment of this Act, and annually thereafter, a large data holder that uses an algorithm, solely or in part, to process or transfer covered data must conduct an impact assessment of such algorithm. (B) IMPACT ASSESSMENT SCOPE. —The impact assessment required under subparagraph (A) shall describe steps the large data holder has taken or will take to mitigate potential harms to an individual, including potential harms related to—	(A) IMPACT ASSESSMENT. — Notwithstanding any other provision of law, not later than [*SLC Note: To be provided*] after the date of enactment of this Act, and annually thereafter, a large data holder that uses an algorithm, solely or in part, to process or transfer covered data must conduct an impact assessment of such algorithm. (B) IMPACT ASSESSMENT SCOPE. — The impact assessment required under subparagraph (A) shall describe steps the large data holder has taken or will take to mitigate potential harms to an individual, including potential harms related to—	(A) IMPACT ASSESSMENT. — Notwithstanding any other provision of law, not later than [___] after the date of enactment of this Act, and annually thereafter, a large data holder that uses an algorithm, solely or in part, to **collect**, process or transfer covered data must conduct an impact assessment of such algorithm. (B) IMPACT ASSESSMENT SCOPE. —The impact assessment required under subparagraph (A) shall describe steps the large data holder has taken or will take to mitigate potential harms to an individual, including potential harms related to—
(i) any individual under the age of **16**; (ii) making or facilitating advertising for housing, education, employment, healthcare, insurance, or credit opportunities; ~~or~~ (iii) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of an individual.	(i) any individual under the age of 16; (ii) making or facilitating advertising for housing, education, employment, healthcare, insurance, or credit opportunities; or (iii) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of an individual.	(i) any individual under the age of **17**. (ii) making or facilitating advertising for housing, education, employment, healthcare, insurance, or credit opportunities. (iii) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of an individual, **including race, color, religion, national origin, gender, sexual orientation, or disability; or** **(iv) disparate impact on the basis of an individual's or class of individuals' race, color, religion, national origin, gender, sexual orientation, or disability status.**
(2) ALGORITHM DESIGN EVALUATION.—Notwithstanding any other provision of law, not later than [SLC Note: To be provided] after the date of enactment of this Act, a covered entity that knowingly develops an algorithm, solely or in part, to process or transfer covered data shall	(2) ALGORITHM DESIGN EVALUATION. — Notwithstanding any other provision of law, not later than [*SLC Note: To be provided]* after the date of enactment of this Act, a covered entity that knowingly develops an algorithm, solely or in part, to process or transfer covered data shall	(2) ALGORITHM DESIGN EVALUATION. —Notwithstanding any other provision of law, not later than [___] after the date of enactment of this Act, a covered entity that knowingly develops an algorithm, solely or in part, to collect, process or transfer covered data shall evaluate the

evaluate the design of the algorithm, including any training data used to develop the algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B). (3) OTHER CONSIDERATIONS. — (A) FOCUS. —In complying with paragraphs (1) or (2), a covered entity may focus the impact assessment or evaluation on any algorithm, or portions of an algorithm, that may reasonably contribute to the risk of the potential harms identified under paragraph (1)(B). (B) EXTERNAL, INDEPENDENT AUDITOR OR RESEARCHER. —A covered entity may utilize an external, independent auditor or researcher to conduct an impact assessment under paragraph (1) or an evaluation under paragraph (2). (C) AVAILABILITY. — (i) IN GENERAL. —A covered entity— (I) shall, not later than [SLC Note: To be provided], submit the impact assessment and evaluation conducted under paragraphs (1) and (2) to the Commission. (II) shall, upon request, make such impact assessment and evaluation available to Congress; and (III) may make such impact assessment and evaluation publicly available in a place that is easily accessible to consumers. (ii) TRADE SECRETS. —A covered entity may redact and segregate any trade secrets (as defined in section 1839 of title 18, United States Code) from public disclosure under this subparagraph.	evaluate the design of the algorithm, including any training data used to develop the algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B). (3) OTHER CONSIDERATIONS. — (A) FOCUS. —In complying with paragraphs (1) or (2), a covered entity may focus the impact assessment or evaluation on any algorithm, or portions of an algorithm, that may reasonably contribute to the risk of the potential harms identified under paragraph (1)(B). (B) EXTERNAL, INDEPENDENT AUDITOR OR RESEARCHER. —A covered entity may utilize an external, independent auditor or researcher to conduct an impact assessment under paragraph (1) or an evaluation under paragraph (2). (C) AVAILABILITY. — (i) IN GENERAL. —A covered entity— (I) shall, not later than [*SLC Note: To be provided],* submit the impact assessment and evaluation conducted under paragraphs (1) and (2) to the Commission. (II) shall, upon request, make such impact assessment and evaluation available to Congress; and (III) may make such impact assessment and evaluation publicly available in a place that is easily accessible to consumers. (ii) TRADE SECRETS. —A covered entity may redact and segregate any trade secrets (as defined in section 1839 of title 18, United States Code) from public disclosure under this subparagraph.	design of the algorithm, including any training data used to develop the algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B). (3) OTHER CONSIDERATIONS. — (A) FOCUS. —In complying with paragraphs (1) or (2), covered entity may focus the impact assessment or evaluation on any algorithm, or portions of an algorithm, that may reasonably contribute to the risk of the potential harms identified under paragraph (1)(B). (B) EXTERNAL, INDEPENDENT AUDITOR OR RESEARCHER. —**To the extent possible,** a covered entity **shall** utilize an external, independent auditor or researcher to conduct an impact assessment under paragraph (1) or an evaluation under paragraph (2). (C) AVAILABILITY. — (i) IN GENERAL. —A covered entity— (I) shall, not later than [___], submit the impact assessment and evaluation conducted under paragraphs (1) and (2) to the Commission. (II) shall, upon request, make such impact assessment and evaluation available to Congress; and (III) may make such impact assessment and evaluation publicly available in a place that is easily accessible to consumers. (ii) TRADE SECRETS. —A covered entity may redact and segregate any trade secrets (as defined in section 1839 of title 18, United States Code) from public disclosure under this subparagraph. **(D) ENFORCEMENT. —The Commission may not use any**

		information obtained solely and exclusively through a covered entity's disclosure of information to the Commission in compliance with this section for any purpose other than enforcing this Act.
(4) GUIDANCE. —Not later than [SLC Note: To be provided] after the date of enactment of this Act, the Commission shall, in consultation with the **Director of the National Institute of Standards and Technology**, publish guidance [**under section 553 of title 5, United States Code,]** regarding compliance with this section.	(4) GUIDANCE. —Not later than [*SLC Note: To be provided]* after the date of enactment of this Act, the Commission shall, in consultation with the Director of the National Institute of Standards and Technology, publish guidance regarding compliance with this section.	(4) GUIDANCE. —Not later than [___] after the date of enactment of this Act, the Commission shall, in consultation with the **Secretary of Commerce or the Secretary's designee**, publish guidance regarding compliance with this section.
(5) RULEMAKING AND EXEMPTION. —The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations as necessary to establish processes by which a large data holder—	(5) RULEMAKING AND EXEMPTION. —The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations as necessary to establish processes by which a large data holder—	(5) RULEMAKING AND EXEMPTION. —The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations as necessary to establish processes by which a large data holder—
(A) shall submit an impact assessment to the Commission under paragraph (3)(C)(i)(I); and (B) may exclude from this subsection any algorithm that presents low or minimal risk for potential for harms to individuals (as identified under paragraph (1)(B)).	(A) shall submit an impact assessment to the Commission under paragraph (3)(C)(i)(I); and (B) may exclude from this subsection any algorithm that presents low or minimal risk for potential for harms to individuals (as identified under paragraph (1)(B)).	(A) shall submit an impact assessment to the Commission under paragraph (3)(C)(i)(I); and (B) may exclude from this subsection any algorithm that presents low or minimal risk for potential for harms to individuals (as identified under paragraph (1)(B)).
(6) STUDY AND REPORT. —	(6) STUDY AND REPORT. —	(6) STUDY AND REPORT. —
(A) STUDY. —The Commission, in consultation with the **Director of the National Institute of Standards and Technology**, shall conduct a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), to review any impact assessment or evaluation submitted under this paragraph. Such study shall include an examination of—	(A) STUDY. —The Commission, in consultation with the Director of the National Institute of Standards and Technology, shall conduct a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), to review any impact assessment or evaluation submitted under this paragraph. Such study shall include an examination of—	(A) STUDY. —The Commission, in consultation with the **Secretary of Commerce or the Secretary's designee**, shall conduct a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), to review any impact assessment or evaluation submitted under this paragraph. Such study shall include an examination of—
(i) best practices for the assessment and evaluation of algorithms; and	(i) best practices for the assessment and evaluation of algorithms; and	(i) best practices for the assessment and evaluation of algorithms; and

(ii) methods to reduce the risk of harm to individuals that may be related to the use of algorithms. (B) REPORT. — (i) INITIAL REPORT. —Not later than 3 years after the date of enactment of this Act, the Commission, in consultation with the **Director of the National Institute of Standards and Technology**, shall submit to Congress a report containing the results of the study conducted under subsection (a), together with recommendations for such legislation and administrative action as the Commission determines appropriate. (ii) ADDITIONAL REPORTS. —Not later than 3 years after submission of the initial report under clause (i), and as the Commission determines necessary thereafter, the Commission shall submit to Congress an updated version of such report.	(ii) methods to reduce the risk of harm to individuals that may be related to the use of algorithms. (B) REPORT. — (i) INITIAL REPORT. —Not later than 3 years after the date of enactment of this Act, the Commission, in consultation with the Director of the National Institute of Standards and Technology, shall submit to Congress a report containing the results of the study conducted under subsection (a), together with recommendations for such legislation and administrative action as the Commission determines appropriate. (ii) ADDITIONAL REPORTS. —Not later than 3 years after submission of the initial report under clause (i), and as the Commission determines necessary thereafter, the Commission shall submit to Congress an updated version of such report.	(ii) methods to reduce the risk of harm to individuals that may be related to the use of algorithms. (B) REPORT. — (i) INITIAL REPORT. —Not later than 3 years after the date of enactment of this Act, the Commission, in consultation with the **Secretary of Commerce or the Secretary's designee**, shall submit to Congress a report containing the results of the study conducted under subsection (a), together with recommendations for such legislation and administrative action as the Commission determines appropriate. (ii) ADDITIONAL REPORTS. —Not later than 3 years after submission of the initial report under clause (i), and as the Commission determines necessary thereafter, the Commission shall submit to Congress an updated version of such report.
Notes: Applies to Covered Entities, Large Data Holders, FTC Covered Entity may not collect (Three Corners Only), process, or transfer Covered Data in a way that discriminates based on protected categories. Exceptions for self-testing and diversity efforts. Large Data Holders using algorithms must conduct impact assessment to evaluate for discrimination. Covered Entities developing algorithms must conduct impact assessments using an external auditor and submit the results to the FTC. FTC works with NIST (Cantwell) or Commerce (Three Corners) to develop guidance on Impact Assessments. FTC is empowered to refer violations of civil rights to appropriate enforcement agencies.		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 205. DATA SECURITY AND PROTECTION OF COVERED DATA. (a) Establishment of Data Security Practices. — (1) IN GENERAL. —A covered entity shall establish, implement, and	SEC. 205. DATA SECURITY AND PROTECTION OF COVERED DATA. (a) ESTABLISHMENT OF DATA SECURITY PRACTICES. — (1) IN GENERAL. —A covered entity shall establish, implement, and	SEC. 208. DATA SECURITY AND PROTECTION OF COVERED DATA. (a) ESTABLISHMENT OF DATA SECURITY PRACTICES. — (1) IN GENERAL. —A covered entity shall establish, implement, and

maintain reasonable data security practices to protect ~~the confidentiality, integrity, and availability of covered data.~~	maintain reasonable data security practices to protect the confidentiality, integrity, and availability of covered data.	maintain reasonable **administrative, technical, and physical** data security practices and procedures to protect **and secure covered data against unauthorized access and acquisition.**
(2) CONSIDERATIONS. —The data security practices required under paragraph (1) shall be appropriate to—	(2) CONSIDERATIONS. —The data security practices required under paragraph (1) shall be appropriate to—	(2) CONSIDERATIONS. —The **reasonable administrative, technical, and physical** data security practices required under paragraph (1) shall be appropriate to—
(A) the size and complexity of the covered entity; (B) the nature and scope of the covered entity's processing of covered data; and	(A) the size and complexity of the covered entity; (B) the nature and scope of the covered entity's processing of covered data; and	(A) the size and complexity of the covered entity; (B) the nature and scope of the covered entity's **collecting**, processing, **or transferring** of covered data;
(C) the volume and nature of the covered data ~~at issue.~~	(C) the volume and nature of the covered data at issue.	(C) the volume and nature of the covered data **collected, processed, or transferred by the covered entity;** **(D) the sensitivity of the covered data collected, processed, or transferred;** **(E) the current state of the art in administrative, technical, and physical safeguards for protecting such covered data; and** **(F) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such covered data in relation to the risks and nature of the covered data.**
(b) Specific Requirements. —The data security practices required under subsection (a) shall include, at a minimum, the following practices:	(b) SPECIFIC REQUIREMENTS. —The data security practices required under subsection (a) shall include, at a minimum, the following practices:	(b) SPECIFIC REQUIREMENTS. —The data security practices required under subsection (a) shall include, at a minimum, the following practices:
(1) ASSESS VULNERABILITIES. —Identifying and assessing any ~~reasonably foreseeable~~ risk to, and vulnerability in, each system maintained by the covered entity that processes or transfers covered data, including unauthorized access to or risks to such covered data, human vulnerabilities, access rights, and the use of service providers. Such activities shall include a plan to receive and respond to unsolicited reports of vulnerabilities by any entity or individual.	(1) ASSESS VULNERABILITIES. —Identifying and assessing any reasonably foreseeable risk to, and vulnerability in, each system maintained by the covered entity that processes or transfers covered data, including unauthorized access to or risks to such covered data, human vulnerabilities, access rights, and the use of service providers. Such activities shall include a plan to receive and respond to unsolicited reports of vulnerabilities by any entity or individual.	(1) ASSESS VULNERABILITIES. —Identifying and assessing any **material internal and external** risk to, and vulnerability in, the security of each system maintained by the covered entity that **collects**, processes or transfers covered data, including unauthorized access to or risks to such covered data, human vulnerabilities, access rights, and the use of service providers. Such activities shall include a plan to receive and respond to unsolicited reports of vulnerabilities by any entity or individual.

(2) PREVENTIVE AND CORRECTION ACTION. —Taking preventive and corrective action to mitigate any risk or vulnerability to covered data identified by the covered entity, which may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software.	(2) PREVENTIVE AND CORRECTION ACTION. —Taking preventive and corrective action to mitigate any risk or vulnerability to covered data identified by the covered entity, which may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software.	(2) PREVENTIVE AND CORRECTIVE ACTION. —Taking preventive and corrective action to mitigate any **reasonably foreseeable** risk or vulnerability to covered data identified by the covered entity, which may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software. **(3) EVALUATION OF PREVENTIVE AND CORRECTIVE ACTION. —Evaluating and making reasonable adjustments to the safeguards described in paragraph (2) in light of any material changes in technology, internal or external threats to covered data, and the covered entity's own changing business arrangements or operations.**
(3) INFORMATION RETENTION AND DISPOSAL. —Disposing of covered data that is required to be deleted by law or is no longer necessary for the purpose for which the data was processed or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section.	(3) INFORMATION RETENTION AND DISPOSAL. —Disposing of covered data that is required to be deleted by law or is no longer necessary for the purpose for which the data was processed or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section.	(4) INFORMATION RETENTION AND DISPOSAL. —Disposing of covered data that is required to be deleted by law or is no longer necessary for the purpose for which the data was **collected**, processed, or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section.
(4) TRAINING. —Training each employee with access to covered data on how to safeguard covered data and updating such training as necessary.	(4) TRAINING. —Training each employee with access to covered data on how to safeguard covered data and updating such training as necessary.	(5) TRAINING. —Training each employee with access to covered data on how to safeguard covered data and updating such training as necessary. **(6) DESIGNATION. —Designating an officer, employee, or employees to**

		maintain and implement such practices.
(c) Regulations. —The Commission may promulgate in accordance with section 553 of title 5, United States Code, technology-neutral, **process-based** regulations that interpret this section. (d) Applicability of Other Information Security Laws.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.) and is in compliance with the information security requirements of such Act, shall be deemed to be in compliance with the requirements of this section with respect to any data covered by such information security requirements.	(c) REGULATIONS. —The Commission may promulgate in accordance with section 553 of title 5, United States Code, technology-neutral, process-based regulations that interpret this section. (d) APPLICABILITY OF OTHER INFORMATION SECURITY LAWS. —A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et 39 seq.), and is in compliance with the information security requirements of such Act, shall be deemed to be in compliance with the requirements of this section with respect to any data covered by such information security requirements.	(c) REGULATIONS. —The Commission may promulgate in accordance with section 553 of title 5, United States Code, technology-neutral regulations to establish processes for complying with this section. (d) APPLICABILITY OF OTHER INFORMATION SECURITY LAWS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), and is in compliance with the information security requirements of such Act, shall be deemed to be in compliance with the requirements of this section with respect to any data covered by such information security requirements.
Notes: Applies to Covered Entities, FTC Covered Entities must adopt data security practices to protect data. The practices must be appropriate to the size of and complexity of the Covered Entity and the nature of the data. Additionally, (Three Corners Only) the practices must take into consideration the sensitivity of the data as well as the cost of protections and technological state of the art. At a minimum, Covered Entities must assess vulnerabilities and take preventative action to mitigate risk, dispose of Covered Data that is no longer necessary (except with Express Affirmative Consent), train employees, and (Three Corners Only) designate an Officer or Employee to implement the practices. FTC is empowered to promulgate technology-neutral processes for compliance.		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 206. GENERAL EXCEPTIONS. (a) General Exceptions. — (1) IN GENERAL. —A covered entity may process or transfer covered data for any of the following purposes, provided that the processing or transfer is reasonably necessary, proportionate, and limited to such purpose:	SEC. 206. GENERAL EXCEPTIONS. (a) GENERAL EXCEPTIONS. — (1) IN GENERAL. — A covered entity may process or transfer covered data for any of the following purposes, provided that the processing or transfer is reasonably necessary, proportionate, and limited to such purpose:	SEC. 209. GENERAL EXCEPTIONS. (a) GENERAL EXCEPTIONS. —A covered entity may **collect**, process, or transfer covered data for any of the following purposes, provided that the **collection**, processing, or transfer is reasonably necessary, proportionate, and limited to such purpose:

(A) To initiate or complete a transaction or fulfill an order or service specifically requested by an individual, including any associated routine administrative activity such as billing, shipping, and accounting. (B) To perform system maintenance, maintain a product or service, perform inventory management or network management, or debug or repair errors that impair the functionality of a service or product provided by the covered entity.	(A) To initiate or complete a transaction or fulfill an order or service specifically requested by an individual, including any associated routine administrative activity such as billing, shipping, and accounting. (B) To perform system maintenance, maintain a product or service, perform inventory management or network management, or debug or repair errors that impair the functionality of a service or product provided by the covered entity.	(1) To initiate or complete a transaction or fulfill an order or service specifically requested by an individual, including any associated routine administrative activity such as billing, shipping, and accounting. (2) **With respect to covered data previously collected in accordance with this Act, notwithstanding this exception**, to perform system maintenance, diagnostics, maintain a product or service **for which such covered data was collected, conduct internal research or analytics to improve products and services**, perform inventory management or network management, or debug or repair errors that impair the functionality of a service or product **for which such covered data was collected** by the covered entity**, except such data shall not be transferred.**
(C) **Subject to paragraph (2),** to detect or respond to a security incident**, provide a secure environment, maintain the safety or security of a product, service, or network,** or fulfill product or service warranty.	(C) Subject to paragraph (2), to detect or respond to a security incident, provide a secure environment, maintain the safety or security of a product, service, or network, or fulfill product or service warranty.	(3) To detect or respond to a security incident or fulfill product or service warranty.
(D) **Subject to paragraph (2),** to protect against malicious, deceptive, fraudulent, or illegal activity.	(D) Subject to paragraph (2), to protect against malicious, deceptive, fraudulent, or illegal activity.	(4) To protect against fraudulent or illegal activity.
(E) To comply with a legal obligation imposed by Federal or State law, or to establish, exercise, or defend legal claims.	(E) To comply with a legal obligation imposed by Federal or State law, or to establish, exercise, or defend legal claims.	(5) To comply with a legal obligation imposed by Federal or State law, or to establish, exercise, or defend legal claims.
(F) To prevent an individual from suffering harm where the covered entity believes in good faith that the individual is at risk of death or serious physical injury.	(F) To prevent an individual from suffering harm where the covered entity believes in good faith that the individual is at risk of death or serious physical injury.	(6) To prevent an individual from suffering harm where the covered entity believes in good faith that the individual is at risk of death or serious physical injury.
(G) To effectuate a product recall pursuant to Federal or State law.	(G) To effectuate a product recall pursuant to Federal or State law.	(7) To effectuate a product recall pursuant to Federal or State law.
(H) To conduct a public or peer-reviewed scientific, historical, or statistical research that—	(H) To conduct a public or peer-reviewed scientific, historical, or statistical research that—	(8) To conduct public or peer-reviewed scientific, historical, or statistical research that—
(i) is in the public interest; (ii) adheres to ~~all applicable ethics and privacy laws; and~~ ~~(iii) is approved, monitored, and governed by an institutional review~~	(i) is in the public interest; (ii) adheres to all applicable ethics and privacy laws; and (iii) is approved, monitored, and governed by an institutional review	(A) is in the public interest; and (B) adheres to **the regulations for human subject research established under part 46 of title 45, Code of**

~~board or other oversight entity that meets standards promulgated by the Commission in accordance with section 553 of title 5, United States Code.~~	board or other oversight entity that meets standards promulgated by the Commission in accordance with section 553 of title 5, United States Code.	**Federal Regulations (or a successor regulations).** **[(9) To cooperate with an Executive agency or a law enforcement official acting under the authority of an Executive or State agency concerning conduct or activity that the Executive agency or law enforcement official reasonably and in good faith believes may violate Federal, State, or local law, or pose a threat to public safety or national security.]**
(2) BIOMETRIC INFORMATION. —For a purpose described in subparagraph (C) or (D) of paragraph (1), a covered entity— **(A) may not transfer biometric information to a third party other than to comply with a legal obligation or to establish, exercise, or defend a legal claim; and** **(B) shall disclose each specific data processing and transfer activity related to biometric information in a clear, conspicuous, and readily accessible manner.**	(2) BIOMETRIC INFORMATION. — For a purpose described in subparagraph (C) or (D) of paragraph (1), a covered entity— (A) may not transfer biometric information to a third party other than to comply with a legal obligation or to establish, exercise, or defend a legal claim; and (B) shall disclose each specific data processing and transfer activity related to biometric information in a clear, conspicuous, and readily accessible manner.	
[(b) Journalism. —Nothing in this Act shall be construed to limit or diminish First Amendment freedoms to gather and publish information guaranteed under the Constitution.]	(b) JOURNALISM. —Nothing in this Act shall be construed to limit or diminish First Amendment freedoms to gather and publish information guaranteed under the Constitution.	(b) JOURNALISM. —Nothing in this Act shall be construed to limit or diminish First Amendment freedoms to gather and publish information guaranteed under the Constitution.
(c) Small Data Exception. —	(c) SMALL DATA EXCEPTION. —	(c) SMALL DATA EXCEPTION. —
(1) IN GENERAL. **— [Sections [102], 202, and 205]** shall not apply in the case of a covered entity that can establish that—	(1) IN GENERAL. —Sections 102, 202(a)(4), and 205(b) shall not apply in the case of a covered entity that can establish that—	(1) IN GENERAL. —Any covered entity that can establish that it met the requirements described in paragraph (2) for the period of the 3 preceding calendar years (or for the period during which the covered entity has been in existence if such period is less than 3 years) shall— (A) **be exempt from compliance with sections 203(a)(4), 208(b)(1)-(3) and (5)-(6), 301(c); and** **(B) at the covered entity's sole discretion, have the option of**

		complying with section 203(a)(2) by, after receiving a verified request from an individual to correct covered data of the individual under such section, deleting such covered data in its entirety instead of making the requested correction.
(A) the covered entity's average annual gross revenues for the period of the 3 preceding calendar years **(or for the period during which the covered entity has been in existence if such period is less than 3 years)** did not exceed **$25,000,000;**	(A) the covered entity's average annual gross revenues for the period of the 3 preceding calendar years (or for the period during which the covered entity has been in existence if such period is less than 3 years) did not exceed $25,000,000.	(2) EXEMPTION REQUIREMENTS. —The requirements of this paragraph are, with respect to a covered entity and a period, the following: (A) The covered entity's average annual gross revenues during the period did not exceed **$41,000,000.**
(B) on average, the covered entity did not annually process the covered data of more than 100,000 individuals**, or devices that identify or are linked or reasonably linkable to 1 or more individuals during such period**; and	(B) on average, the covered entity did not annually process the covered data of more than 100,000 individuals, or devices that identify or are linked or reasonably linkable to 1 or more individuals during such period; and	(B) The covered entity**, on average,** did not annually collect or process the covered data of more than [100,000] individuals during the period **beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose is deleted within 90 days**.
(C) the covered entity did not derive more than 50 percent of its annual revenues from transferring covered data during such a period.	(C) the covered entity did not derive more than 50 percent of its annual revenues from transferring covered data during such period.	(C) The covered entity did not derive more than 50 percent of its revenue from transferring covered data during any year **(or part of a year if the covered entity has been in existence for less than 1 year)** that occurs during the period.
(2) DEFINITION.—For purposes of this section, the term "revenue" as it relates to any covered entity that is not organized to carry on business for its own profit or that of their members, means the gross receipts the covered entity received in whatever form from all sources without subtracting any costs or expenses, and includes contributions, gifts, grants, dues or other assessments, income from investments, or proceeds from the sale of real or personal property.	(2) DEFINITION. —For purposes of this section, the term ''revenue'' as it relates to any covered entity that is not organized to carry on business for its own profit or that of their members, means the gross receipts the covered entity received in whatever form from all sources without subtracting any costs or expenses, and includes contributions, gifts, grants, dues or other assessments, income from investments, or proceeds from the sale of real or personal property.	(3) DEFINITION.—For purposes of this section, the term "revenue" as it relates to any covered entity that is not organized to carry on business for its own profit or that of their members, means the gross receipts the covered entity received in whatever form from all sources without subtracting any costs or expenses, and includes contributions, gifts, grants, dues or other assessments, income from investments, or proceeds from the sale of real or personal property.
Notes: Applies to Covered Entity		

Exceptions to data collection, processing, and transfer prohibitions. Permitted to initiate or complete transactions, to perform system maintenance, conduct network security, fulfill warranty and product service requests, comply with legal obligations, prevent harm, initiate product recall, conduct research, or (Three Corners Only) comply with law enforcement. Cantwell would limit the exceptions for Biometric data. Cantwell exempts Small Data from Data Minimization (Sec. 102), Individual Control (Sec. 202), and Data Security (Sec. 205) provisions. Defined as less than $25m revenue, processes fewer than 100,000 individuals' data, and does not get more than half of its revenue from transferring data. Three Corners exempts Small Data from Data Export (Sec. 203(a)(4)), specific vulnerability assessments (Sec. 208(b)(1)-(6)), and maintaining a Chief Privacy Officer (Sec. 301(c)) Covered Entities that receive more than 50% of revenue from transferring data are not exempted.

Cantwell	**Three Corners**
--	SEC. 210. UNIFIED OPT-OUT MECHANISMS. (a) For the rights established under sections 204(c)(2), 204(d)(2), and section 206 (c)(3)(D), not later than 18 months after the date of enactment of this Act, the Commission shall initiate and finalize a feasibility study on the creation of a privacy protective, centralized mechanism for individuals to exercise all such rights through a single interface. (b) RULEMAKING. —If the Commission determines that a centralized mechanism is feasible under subparagraph (a) for any or all of the rights established, the Commission shall issue a rule under section 553 of title 5, United States Code, establishing 1 or more acceptable mechanisms as described in subparagraph (a) for a covered entity to utilize to allow an individual to make such opt out designations with respect to covered data related to such individual.
Notes: Applies to FTC. Directs FTC to conduct rulemaking to determine feasibility and implement centralized acceptable opt-out mechanism. Cantwell establishes this in Section 203.	

CORPORATE ACCOUNTABILITY

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 301. EXECUTIVE RESPONSIBILITY. (a) In General.—Beginning 1 year after the date of enactment of this Act, the chief executive officer of a large data	SEC. 301. EXECUTIVE RESPONSIBILITY. (a) IN GENERAL. —Beginning 1 year after the date of enactment of this Act, the chief executive officer of a large	SEC. 301. EXECUTIVE RESPONSIBILITY. (a) IN GENERAL.—Beginning 1 year after the date of enactment of this Act, the chief executive officer of a large

holder (or, if the large data holder does not have a chief executive officer, the highest ranking officer of the large data holder) and each privacy officer and data security officer of such large data holder shall annually certify to the Commission, in a manner specified by the Commission, that the entity maintains—	data holder (or, if the large data holder does not have a chief executive officer, the highest-ranking officer of the large data holder) and each privacy officer and data security officer of such large data holder shall annually certify to the Commission, in a manner specified by the Commission, that the entity maintains—	data holder (or, if the large data holder does not have a chief executive officer, the highest ranking officer of the large data holder) and each privacy officer and data security officer of such large data holder shall annually certify to the Commission, by regulation under section 553 of title 5, United States Code, in a manner specified by the Commission, that the entity maintains—
(1) reasonable internal controls to comply with this Act; and (2) reporting structures to ensure that such certifying officers are involved in and are responsible for decisions that impact the entity's compliance with this Act.	(1) reasonable internal controls to comply with this Act; and (2) reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this Act.	(1) reasonable internal controls to comply with this Act; and (2) reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this Act.
(b) Requirements. —A certification submitted under subsection (a) shall be based on a review of the effectiveness of a large data holder's internal controls and reporting structures that is conducted by the certifying officers not more than 90 days before the submission of the certification.	(b) REQUIREMENTS. —A certification submitted under subsection (a) shall be based on a review of the effectiveness of a large data holder's internal controls and reporting structures that is conducted by the certifying officers not more than 90 days before the submission of the certification.	(b) REQUIREMENTS. —A certification submitted under subsection (a) shall be based on a review of the effectiveness of a large data holder's internal controls and reporting structures that is conducted by the certifying officers not more than 90 days before the submission of the certification.
(c) Designation of Privacy and Data Security Officer. — (1) IN GENERAL. —A covered entity shall designate—	(c) DESIGNATION OF PRIVACY AND DATA SECURITY OFFICER. — (1) IN GENERAL. —A covered entity shall designate—	(c) DESIGNATION OF PRIVACY AND DATA SECURITY OFFICER. — (1) IN GENERAL. —A covered entity shall designate—
(A) 1 or more qualified employees as privacy officers; and (B) 1 or more qualified employees (in addition to any employee designated under subparagraph (A)) as data security officers.	(A) 1 or more qualified employees as privacy officers; and (B) 1 or more qualified employees (in addition to any employee designated under subparagraph (A)) as data security officers.	(A) 1 or more qualified employees as privacy officers; and (B) 1 or more qualified employees (in addition to any employee designated under subparagraph (A)) as data security officers.
(2) REQUIREMENTS FOR OFFICERS. —An employee who is designated by a covered entity 30 as a privacy officer or a data security officer shall, at a minimum—	(2) REQUIREMENTS FOR OFFICERS. —An employee who is designated by a covered entity as a privacy officer or a data security officer shall, at a minimum—	(2) REQUIREMENTS FOR OFFICERS. —An employee who is designated by a covered entity as a privacy officer or a data security officer shall, at a minimum—

(A) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this Act; (B) facilitate the covered entity's ongoing compliance with this Act.	(A) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this Act; and (B) facilitate the covered entity's ongoing compliance with this Act.	(A) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this Act; and (B) facilitate the covered entity's ongoing compliance with this Act. **(3) ADDITIONAL REQUIREMENTS FOR LARGE DATAHOLDERS. —A large data holder shall designate at least 1 of the officers described in paragraph (1) of this subsection to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the requirements in paragraph (2), either directly or through a supervised designee or designees—** **(A) establish processes to periodically review and update the privacy and security policies, practices, and procedures of the large data holder, as necessary;** **(B) conduct regular and comprehensive audits to ensure the policies, practices, and procedures of the large data holder work to ensure the company is in compliance with all applicable laws;** **(C) develop a program to educate and train employees about compliance requirements;** **(D) maintain updated, accurate, clear, and understandable records of all privacy and data security practices undertaken by the large data holder; and** **(E) serve as the point of contact between the large data holder and enforcement authorities.**
(d) Large Data Holder Privacy Impact Assessments. — (1) IN GENERAL. —Not later than 1 year after the date of enactment of this Act or 1 year after the date that a	(d) LARGE DATA HOLDER PRIVACY IMPACT ASSESSMENTS. — (1) IN GENERAL. —Not later than 1 year after the date of enactment of this Act or 1 year after the	(d) LARGE DATA HOLDER PRIVACY IMPACT ASSESSMENTS. — (1) IN GENERAL. —Not later than 1 year after the date of enactment of this Act or 1 year after the date that a

covered entity first meets the definition of large data holder, whichever is earlier, and biennially thereafter, each large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data processing and transfer practices against the potential adverse consequences of such practices to individual privacy. (2) ASSESSMENT REQUIREMENTS. —A privacy impact assessment required under paragraph (1) shall be— (A) reasonable and appropriate in scope given— (i) the nature of the covered data processed or transferred by the large data holder; (ii) the volume of the covered data processed or transferred by the large data holder; and (iii) the potential risks posed to the privacy of individuals by the processing and transfer of covered data by the large data holder; (B) documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under paragraph (1); and (C) approved by the privacy officer of the large data holder.	date that a covered entity first meets the definition of large data holder, whichever is earlier, and biennially thereafter, each large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data processing and transfer practices against the potential adverse consequences of such practices to individual privacy. (2) ASSESSMENT REQUIREMENTS. —A privacy impact assessment required under paragraph (1) shall be— (A) reasonable and appropriate in scope given— (i) the nature of the covered data processed or transferred by the large data holder; (ii) the volume of the covered data processed or transferred by the large data holder; and (iii) the potential risks posed to the privacy of individuals by the processing and transfer of covered data by the large data holder; (B) documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under paragraph (1); and (C) approved by the privacy officer of the large data holder.	covered entity first meets the definition of large data holder, whichever is earlier, and biennially thereafter, each large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data **collecting**, processing, and transfer practices against the potential adverse consequences of such practices to individual privacy. (2) ASSESSMENT REQUIREMENTS. —A privacy impact assessment required under paragraph (1) shall be— (A) reasonable and appropriate in scope given— (i) the nature of the covered data **collected**, processed, and transferred by the large data holder; (ii) the volume of the covered data **collected**, processed, and transferred by the large data holder; and (iii) the potential risks posed to the privacy of individuals by the **collecting**, processing, and transfer of covered data by the large data holder; (B) documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under paragraph (1); and (C) approved by the privacy officer of the large data holder. (3) ADDITIONAL FACTORS TO INCLUDE IN ASSESSMENT. —In assessing the privacy risks, the large data holder may include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure covered data.
Notes: Applies to Covered Entities, Large Data Holders		

Large Data Holders must have CEO certify that there are reasonable internal controls and reporting structures.

Covered Entities must designate privacy officers. Three Corners requires Large Data Holders to have at least one of those officers report to the CEO.

Large Data Holders must conduct annual Privacy Impact Assessments

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES. (a) Service Providers. —A service provider— (1) shall not process service provider data for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider, except that a service provider may process data to comply with a legal obligation or the establishment, exercise, or defense of legal claims; (2) shall not transfer service provider data to a third party without the affirmative express consent, obtained by the covered entity, of the individual to whom the service provider data is linked or reasonably linkable; (3) shall delete or de-identify service provider data as soon as practicable after the contractually agreed upon end of the provision of services; (4) shall be exempt from the requirements of sections 202 and 203 with respect to service provider data, but shall, to the extent practicable—	SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES. (a) SERVICE PROVIDERS. —A service provider— (1) shall not process service provider data for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider, except that a service provider may process data to comply with a legal obligation or the establishment, exercise, or defense of legal claims; (2) shall not transfer service provider data to a third party without the affirmative express consent, obtained by the covered entity, of the individual to whom the service provider data is linked or reasonably linkable; (3) shall delete or de-identify service provider data as soon as practicable after the contractually agreed upon end of the provision of services; (4) shall be exempt from the requirements of sections 202 and 203 with respect to service provider data, but shall, to the extent practicable—	SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES. (a) SERVICE PROVIDERS. —A service provider— (1) shall not **collect or** process service provider data for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider, except that a service provider may process data to comply with a legal obligation or the establishment, exercise, or defense of legal claims; (2) shall not transfer service provider data to a third party, **other covered entity, or another service provider** without the affirmative express consent, obtained by the covered entity **with the direct relationship to the individual**, of the individual to whom the service provider data is linked or reasonably linkable; (3) shall delete or de-identify service provider data as soon as practicable after the earlier of— (A) the contractually agreed upon end of the provision of services; and (**B) when such data no longer serves any legitimate purpose under the contractual arrangement with the covered entity;** (4) shall be exempt from the requirements of sections 203 and 204 with respect to service provider data, but shall, to the extent practicable—

(A) assist the covered entity from which it received the service provider data in fulfilling requests to exercise any right granted under such sections; and (B) upon receiving notice from a covered entity of a verified request made under such sections **to delete, de-identify, or correct service provider data held by the service provider, delete, de-identify, or correct such data, as applicable; and**	(A) assist the covered entity from which it received the service provider data in fulfilling requests to exercise any right granted under such sections; and (B) upon receiving notice from a covered entity of a verified request made under such sections to delete, de-identify, or correct service provider data held by the service provider, delete, de-identify, or correct such data, as applicable; and	(A) assist the covered entity from which it received the service provider data in fulfilling requests to exercise any right granted under such sections; and (B) upon receiving notice from a covered entity of a verified request made under such sections **related to service provider data transferred to the service provider by the covered entity, execute such request; and**
(5) **shall be exempt from the requirements of section 102 with respect to service provider data but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act (except as provided in paragraph (4)).**	(5) shall be exempt from the requirements of section 102 with respect to service provider data, but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act (except as provided in paragraph (4)).	(5) **shall have the same responsibilities and obligations as a covered entity with respect to such data under all provisions of this Act except as otherwise provided in this section.**
(b) Third Parties. —A third party—	(b) THIRD PARTIES. —A third party—	(b) THIRD PARTIES. —A third party—
(1) shall not process third party data for a processing purpose inconsistent with the expectations of a reasonable individual; (2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third party data regarding the expectations of a reasonable individual, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and (3) shall be exempt from the requirements of **section** [**203**] [SLC Note: Review cross reference] with respect to third party data but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.	(1) shall not process third party data for a processing purpose inconsistent with the expectations of a reasonable individual; (2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third party data regarding the expectations of a reasonable individual, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and (3) shall be exempt from the requirements of section 203(a) with respect to third party data but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.	(1) shall not process third party data for a processing purpose inconsistent with the expectations of a reasonable individual; (2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third-party data regarding the expectations of a reasonable individual, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and (3) shall be exempt from the requirements of **section 204** with respect to third party data but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.
(c) Additional Obligations on Covered Entities. —	(c) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES. —	(c)ADDITIONAL OBLIGATIONS ON COVERED ENTITIES. —

(1) IN GENERAL. —A covered entity 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 [SLC Note: To be provided] after the date of enactment of this Act, the Commission shall publish guidance regarding compliance with this subsection. Such guidance shall, to the extent practicable, minimize unreasonable burdens on small- and medium-sized covered entities.	(1) IN GENERAL. —A covered entity 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 [*SLC Note: To be provided]* after the date of enactment of this Act, the Commission shall publish guidance regarding compliance with this subsection. Such guidance shall, to the extent practicable, minimize unreasonable burdens on small- and medium-sized covered entities.	(1) IN GENERAL. —A covered entity 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 [___] after the date of enactment of this Act, the Commission shall publish guidance regarding compliance with this subsection. Such guidance shall, to the extent practicable, minimize unreasonable burdens on small- and medium-sized covered entities.
Notes: Applies to Service Providers, Third Parties, and Covered Entities Service Providers prohibited from collecting (Three Corners Only) or process data for any processing purpose that is not performed on behalf of the relevant Covered Entity. Service Providers may not transfer Covered Data except with Affirmative Consent obtained from the individual by the relevant Covered Entity. Service Providers must delete data as soon as possible after completing services or (Three Corners Only) when it no longer serves legitimate purpose. Service Providers are exempt from individual access requests but must assist Covered Entities who are subject to those request. Must delete, de-identify, or correct data when requested by Covered Entity. Third Parties prohibited from processing third-party data except as consistent with expectations. Exempt from individual access requests for third-party data but must comply with requests for other Covered Data. Covered Entities must take reasonable precautions when choosing Service Providers or transferring data to Third Parties.		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 304. TECHNICAL COMPLIANCE PROGRAMS. (a) In General. —Not later than 120 days after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish a process for the proposal and approval of technical compliance programs specific to any technology, product, service, or method used by a	SEC. 304. TECHNICAL COMPLIANCE PROGRAMS. (a) IN GENERAL. —Not later than 120 days after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish a process for the proposal and approval of technical compliance programs specific to any technology, product, service, or method	SEC. 303. TECHNICAL COMPLIANCE PROGRAMS. (a) IN GENERAL. —Not later than 120 days after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish a process for the proposal and approval of technical compliance programs specific to any technology, product, service, or method

covered entity to process or transfer covered data. (b) Scope of Programs. —The technical compliance programs established under this section shall, with respect to a technology, product, service, or method used by a covered entity to process or transfer covered data— (1) establish guidelines for compliance with this Act; (2) meet or exceed the requirements of this Act; and (3) be made publicly available to any individual whose covered data is processed or transferred using such technology, product, service, or method. (c) Approval Process. — (1) IN GENERAL. —Any request for approval of a technical compliance program may be submitted to the Commission by any person, including a covered entity, a representative of a covered entity, an association of covered entities, or a public interest group or organization. (2) EXPEDITED RESPONSE TO REQUESTS. —The Commission shall act upon a request for the proposal and approval of a technical compliance program not later than 180 days after the filing of the request and shall set forth publicly in writing its conclusions with regard to such request. (d) Right to Appeal. —Final action by the Commission on a request for approval of [a technical compliance program], or the failure to act within the 180 day period after a request for approval of [a technical compliance program] is made under subsection (c), may be appealed to a district court of the United States of appropriate	used by a covered entity to process or transfer covered data. (b) SCOPE OF PROGRAMS. —The technical compliance programs established under this section shall, with respect to a technology, product, service, or method used by a covered entity to process or transfer covered data— (1) establish guidelines for compliance with this Act; (2) meet or exceed the requirements of this Act; and (3) be made publicly available to any individual whose covered data is processed or transferred using such technology, product, service, or method. (c) APPROVAL PROCESS. — (1) IN GENERAL. —Any request for approval of a technical compliance program may be submitted to the Commission by any person, including a covered entity, a representative of a covered entity, an association of covered entities, or a public interest group or organization. (2) EXPEDITED RESPONSE TO REQUESTS. —The Commission shall act upon a request for the proposal and approval of a technical compliance program not later than 180 days after the filing of the request and shall set forth publicly in writing its conclusions with regard to such request. (d) RIGHT TO APPEAL. —Final action by the Commission on a request for approval of a technical compliance program, or the failure to act within the 180 day period after a request for approval of a technical compliance program is made under subsection (c), may be appealed to a district court of the United States of appropriate	used by a covered entity to **collect**, process, or transfer covered data. (b) SCOPE OF PROGRAMS. —The technical compliance programs established under this section shall, with respect to a technology, product, service, or method used by a covered entity to **collect**, process, or transfer covered data— (1) establish guidelines for compliance with this Act; (2) meet or exceed the requirements of this Act; and (3) be made publicly available to any individual whose covered data is **collected**, processed, or transferred using such technology, product, service, or method. (c)APPROVAL PROCESS. — (1) IN GENERAL. —Any request for approval of a technical compliance program may be submitted to the Commission by any person, including a covered entity, a representative of a covered entity, an association of covered entities, or a public interest group or organization. (2) EXPEDITED RESPONSE TO REQUESTS. —The Commission shall act upon a request for the proposal and approval of a technical compliance program not later than 180 days after the filing of the request and shall set forth publicly in writing its conclusions with regard to such request. (d) RIGHT TO APPEAL. —Final action by the Commission on a request for approval of a technical compliance program, or the failure to act within the 180-day period after a request for approval of a technical compliance program is made under subsection (c), may be appealed to a **Federal** district court of the United States of

jurisdiction as provided for in section 702 of title 5, United States Code.	jurisdiction as provided for in section 702 of title 5, United States Code.	appropriate jurisdiction as provided for in section 702 of title 5, United States Code.
(e) Effect on Enforcement. —	(e) EFFECT ON ENFORCEMENT. —	(e)EFFECT ON ENFORCEMENT. —
(1) IN GENERAL. —Prior to commencing an investigation or enforcement action against any covered entity under this Act, the Commission shall consider the covered entity's history of compliance with any [technical compliance] program approved under this section and any action taken by the covered entity to remedy noncompliance with such program.	(1) IN GENERAL. —Prior to commencing an investigation or enforcement action against any covered entity under this Act, the Commission shall consider the covered entity's history of compliance with any technical compliance program approved under this section and any action taken by the covered entity to remedy noncompliance with such program.	(1) IN GENERAL. —Prior to commencing an investigation or enforcement action against any covered entity under this Act, the Commission **and state Attorney General** shall consider the covered entity's history of compliance with any technical compliance program approved under this section and any action taken by the covered entity to remedy noncompliance with such program. **If such enforcement action described in Sec. 403 is commenced, the court shall take into consideration the covered entity's history of compliance with any technical compliance program approved under this section and any action taken by the covered entity to remedy noncompliance with such program.**
(2) COMMISSION AUTHORITY. — Approval of a [technical] compliance program shall not limit the authority of the Commission, including the Commission's authority to commence an investigation or enforcement action against any covered entity under this Act or any other Act.	(2) COMMISSION AUTHORITY. — Approval of a technical compliance program shall not limit the authority of the Commission, including the Commission's authority to commence an investigation or enforcement action against any covered entity under this Act or any other Act.	(2) COMMISSION AUTHORITY. — Approval of a technical compliance program shall not limit the authority of the Commission, including the Commission's authority to commence an investigation or enforcement action against any covered entity under this Act or any other Act.
Notes: Applies to FTC, AGs (Three Corners Only) FTC to promulgate regulations to establish a technical compliance program and guidelines for compliance. Directs Commission and AGs (Three Corners Only) to consider past compliance when bringing enforcement actions.		

Cantwell	**Three Corners**
--	SEC. 304. COMMISSION APPROVED COMPLIANCE GUIDELINES. (a) APPLICATION FOR COMPLIANCE GUIDELINE APPROVAL. — (1) IN GENERAL. —A covered entity that is not a third-party collecting entity and meets the requirements of section

	210(c), or a group of such covered entities, may apply to the Commission for approval of 1 or more sets of compliance guidelines governing the collection, processing, and transfer of covered data by the covered entity or group of covered entities. (2) APPLICATION REQUIREMENTS. —Such application shall include— (A) a description of how the proposed guidelines will meet or exceed the requirements of this Act; (B) a description of the entities or activities the proposed set of compliance guidelines is designed to cover; (C) a list of the covered entities, if any are known at the time of application, that intend to adhere to the compliance guidelines; and (D) a description of how such covered entities will be independently assessed for adherence to such compliance guidelines, including the independent organization not associated with any of the covered entities that may participate in guidelines that will administer such guidelines. (3) COMMISSION REVIEW. — (A) INITIAL APPROVAL. — (i) PUBLIC COMMENT PERIOD. —As soon as feasible after the receipt of proposed guidelines submitted pursuant to paragraph (2), the Commission shall provide an opportunity for public comment on such compliance guidelines. (ii) APPROVAL. —The Commission shall approve an application regarding proposed guidelines under paragraph (2) if the applicant demonstrates that the compliance guidelines— (I) meet or exceed the requirements of this Act; and (II) provide for the regular review and validation by an independent organization not associated with any of the covered entities that may participate in the guidelines and that is approved by the Commission to conduct such reviews of the compliance guidelines of the covered entity or entities to ensure that the covered entity or entities continue to meet or exceed the requirements of this Act; and (III) include a means of enforcement if a covered entity does not meet or exceed the requirements in the guidelines, which may include referral to the Commission for enforcement consistent with section 401 or referral to the appropriate State attorney general for enforcement consistent with section 402.

	(iii) TIMELINE. —Within **[**180 days**]** of receiving an application regarding proposed guidelines under paragraph (2), the Commission shall issue a determination approving or denying the application and providing its reasons for approving or denying such application. (B) APPROVAL OF MODIFICATIONS. — (i) IN GENERAL. —If the independent organization administering a set of guidelines makes material changes to guidelines previously approved by the Commission, the independent organization must submit the updated guidelines to the Commission for approval. (ii) TIMELINE. —The Commission shall approve or deny any material change to the guidelines within **[**90 days**]** after receipt of the submission for approval. (b) WITHDRAWAL OF APPROVAL.—If at any time the Commission determines that the guidelines previously approved no longer meet the requirements of this Act or a regulation promulgated under this Act or that compliance with the approved guidelines is insufficiently enforced by the independent organization administering the guidelines, the Commission shall notify the covered entities or group of such entities and the independent organization of its intention to withdraw approval of such guidelines and the basis for doing so. Upon receipt of such notice, the covered entity or group of such entities and the independent organization may cure any alleged deficiency with the guidelines or the enforcement of such guidelines within **[**90**]** days and submit the proposed cure or cures to the Commission. If such cures are approved by the Commission, then the Commission may not withdraw approval of such guidelines on the basis of such determination. (c) DEEMED COMPLIANCE. —A covered entity that is eligible to participate, and participates, in, guidelines approved under this section shall be deemed in compliance with this Act if it is in compliance with such guidelines. If such covered entity is not in compliance with guidelines approved under this section, that covered entity is subject to enforcement under section 401, 402, 403 of this Act.
Notes: Applies to Covered Entities (Excluding Third-Party Collecting Entities), FTC Not included in Cantwell. Creates a process for Covered Entities to apply for certification of guidelines that deem compliance with the Act.	

ENFORCEMENT

Cantwell	Cantwell Amendment	Three Corners
SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. (a) New Bureau. — (1) IN GENERAL. —The Commission shall establish within the Commission a new bureau comparable in structure, size, organization, and authority to the existing Bureaus within the Commission related to consumer protection and competition. (2) MISSION. —The mission of the bureau established under this subsection shall be to assist the Commission in exercising the Commission's authority under this Act and related authorities. (3) TIMELINE. —The bureau shall be established, staffed, and fully operational not later than 1 year after the date of enactment of this Act.	SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. (a) NEW BUREAU. — (1) IN GENERAL. —The Commission shall establish within the Commission a new bureau com25 parable in structure, size, organization, and authority to the existing Bureaus within the Commission related to consumer protection and competition. (2) MISSION. —The mission of the bureau established under this subsection shall be to assist the Commission in exercising the Commission's authority under this Act and related authorities. (3) TIMELINE. —The bureau shall be established, staffed, and fully operational not later than 1 year after the date of enactment of this Act.	SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. (a) NEW BUREAU. — (1) IN GENERAL. —The Commission shall establish within the Commission a new bureau comparable in structure, size, organization, and authority to the existing Bureaus within the Commission related to consumer protection and competition. (2) MISSION. —The mission of the bureau established under this subsection shall be to assist the Commission in exercising the Commission's authority under this Act and related authorities. (3) TIMELINE. —The bureau shall be established, staffed, and fully operational not later than 1 year after the date of enactment of this Act. **(b) OFFICE OF BUSINESS MENTORSHIP. —The Director of the Bureau of Privacy shall establish within the Bureau an Office of Business Mentorship to provide guidance and consultation to covered entities regarding compliance with this Act. Covered entities may petition the Commission through this office for tailored guidance as to how to comply with the requirements of this Act.**
(b) Enforcement by the Federal Trade Commission. — (1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. —A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade	(b) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. — (1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. —A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade	(c) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. — (1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. —A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade

Commission Act (15 U.S.C. 57a(a)(1)(B)). (2) POWERS OF COMMISSION. — (A) IN GENERAL. —Except as provided in paragraphs (3), (4) [, and (5)], the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. (B) PRIVILEGES AND IMMUNITIES. —Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 36 41 et seq.). **(3) INDEPENDENT LITIGATION AUTHORITY. —** **(A) IN GENERAL. —The Commission may commence, defend, or intervene in, and supervise the litigation of any civil action under this subsection (including an action to recover a civil penalty) and any appeal of such action in the name of the Commission by any attorney of the Commission that is designated by the Commission for such purpose.** **(B) NOTIFICATION. —Not later than [SLC Note: To be provided] after taking an action under subparagraph (A), the Commission shall notify the Attorney General of the United States of any such action and may consult with the Attorney General with respect to any such**	Commission Act (15 U.S.C. 57a(a)(1)(B)). (2) POWERS OF THE COMMISSION. — (A) IN GENERAL. —Except as provided in paragraphs (3), (4), and (5), the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. (B) PRIVILEGES AND IMMUNITIES. —Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.). (3) INDEPENDENT LITIGATION AUTHORITY. — (A) IN GENERAL. —The Commission may commence, defend, or intervene in, and supervise the litigation of any civil action under this subsection (including an action to recover a civil penalty) and any appeal of such action in the name of the Commission by any attorney of the Commission that is designated by the Commission for such purpose. (B) NOTIFICATION. —Not later than [*SLC Note: To be provided*] after taking an action under subparagraph (A), the Commission shall notify the Attorney General of the United States of any such action and may consult with the Attorney General with respect to any such action or request the	Commission Act (15 U.S.C. 57a(a)(1)(B)). (2) POWERS OF COMMISSION. — (A) IN GENERAL. —Except as provided in paragraphs (3), (4), and (5), the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. (B) PRIVILEGES AND IMMUNITIES. —Any person who violates this Act, or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

action or request the Attorney General on behalf of the Commission to commence, defend, or intervene in any such action.	Attorney General on behalf of the Commission to commence, defend, or intervene in any such action.	
[(4) LIMITING CERTAIN ACTIONS UNRELATED TO THIS ACT. —If the Commission brings an action under paragraph (1) with respect to conduct that is alleged to violate this Act or a regulation promulgated under this Act, the Commission may not seek a cease-and-desist order under section 5(b) of the Federal Trade Commission Act (15 U.S.C. 45(b)) on the grounds that such conduct constitutes an unfair or deceptive act or practice.]	(4) LIMITATION OF ACTIONS. —If the Commission brings an action under paragraph (1) with respect to conduct that is alleged to violate this Act or a regulation promulgated under this Act, the Commission may not seek a cease and desist order under section 5(b) of the Federal Trade Commission Act (15 U.S.C. 45(b)) against the same entity for the same conduct on the grounds that such conduct constitutes an unfair or deceptive act or practice.	(3) LIMITING CERTAIN ACTIONS UNRELATED TO THIS ACT. —If the Commission brings an action under paragraph (1) with respect to conduct that is alleged to violate this Act or a regulation promulgated under this Act, the Commission may not seek a cease-and-desist order under section 5(b) of the Federal Trade Commission Act (15 U.S.C. 45(b)) to stop that same conduct on the grounds that such conduct constitutes an unfair or deceptive act or practice.
[(5) COMMON CARRIERS.— Notwithstanding section (4), (5)(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act and the regulations promulgated under this Act, in the same manner provided in subsections (1), (2), (3), [and (4)] of this subsection, with respect to common carriers subject to title II of the Communications Act of 20 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended.]	(5) COMMON CARRIERS. — Notwithstanding section (4), (5)(a)(2), or of the Federal Trade Com14 mission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act and the regulations promulgated under this Act, in the same manner provided in subsections (1), (2), (3), and (4) of this subsection, with respect to common carriers subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended.	(4) COMMON CARRIERS.— Notwithstanding section (4),(5)(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act and the regulations promulgated under this Act, in the same manner provided in subsections (1), (2), (3), and (5) of this subsection, with respect to common carriers subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended.
(6) DATA PRIVACY AND SECURITY VICTIMS RELIEF FUND. —	(6) DATA PRIVACY AND SECURITY VICTIMS RELIEF FUND. —	(5) DATA PRIVACY AND SECURITY VICTIMS RELIEF FUND. —
(A) ESTABLISHMENT OF VICTIMS RELIEF FUND. —There is established in the Treasury of the United States a separate fund to be known as the “Privacy and Security Victims Relief Fund” (referred to in this paragraph as the “Victims Relief Fund”).	(A) ESTABLISHMENT OF VICTIMS RELIEF FUND. —There is established in the Treasury of the United States a separate fund to be known as the ‘‘Privacy and Security Victims Relief Fund’’ (referred to in this paragraph as the “Victims Relief Fund”).	(A) ESTABLISHMENT OF VICTIMS RELIEF FUND. —There is established in the Treasury of the United States a separate fund to be known as the “Privacy and Security Victims Relief Fund” (referred to in this paragraph as the “Victims Relief Fund”).
(B) DEPOSITS. —	(B) DEPOSITS. —	(B) DEPOSITS. —
(i) DEPOSITS FROM THE COMMISSION. —The Commission shall deposit into the Victims Relief	(i) DEPOSITS FROM THE COMMISSION. —The Commission shall deposit into the Victims Relief	(i) DEPOSITS FROM THE COMMISSION.—The Commission shall deposit into the Victims Relief

Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act.	Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Commission commences to enforce this Act, or a regulation promulgated under this Act.	Fund the amount of any civil penalty obtained against any covered entity **or any other relief the Commission obtains to provide redress, payments or compensation, or other monetary relief to individuals that cannot be located or the payment of which would otherwise not be practicable** in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act.
(ii) DEPOSITS FROM THE ATTORNEY GENERAL OF THE UNITED STATES. —The Attorney General of the United States shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act, or a regulation promulgated under this Act.	(ii) DEPOSITS FROM THE ATTORNEY GENERAL OF THE UNITED STATES. —The Attorney General of the United States shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.	(ii) DEPOSITS FROM THE ATTORNEY GENERAL OFTHE UNITED STATES.—The Attorney General of the United States shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any covered entity **or any other relief the Commission obtains to provide redress, payments or compensation, or other monetary relief to individuals that cannot be located or the payment of which would otherwise not be practicable** in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.
(C) USE OF FUND AMOUNTS. —	(C) USE OF FUND AMOUNTS. —	(C) USE OF FUND AMOUNTS. —
(i) AVAILABILITY TO THE COMMISSION. —Notwithstanding section **3302 of title 37**, United States Code, amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which ~~civil penalties~~ have been obtained under this Act.	(i) AVAILABILITY TO THE COMMISSION. —Notwithstanding section 3302 of title 31, United States Code, amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been obtained under this Act.	(i) AVAILABILITY TO COMMISSION. —Notwithstanding section **3302 of title 31**, United States Code, amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which **relief** has been obtained under this Act.
(ii) OTHER PERMISSIBLE USES. —To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of—	(ii) OTHER PERMISSIBLE USES. —To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of—	(ii) OTHER PERMISSIBLE USES. —To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of—

~~(I) consumer or business education relating to privacy and security; or~~ (II) engaging in technological research that the Commission considers necessary to enforce this Act. (D) AMOUNTS NOT SUBJECT TO APPORTIONMENT. — Notwithstanding any other provision of law, amounts in the Victims Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.	(I) consumer or business education relating to privacy and security; or (II) engaging in technological research that the Commission considers necessary to enforce this Act. (D) AMOUNTS NOT SUBJECT TO APPORTIONMENT. — Notwithstanding any other provision of law, amounts in the Victims Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.	**(I) funding the activities of the Office of Business Mentorship established under subsection (b); or** (II) engaging in technological research that the Commission considers necessary to enforce this Act. (D) AMOUNTS NOT SUBJECT TO APPORTIONMENT. — Notwithstanding any other provision of law, amounts in the Victims Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.
Notes: Enforcement by the FTC. The FTC is directed to establish a new Bureau to enforce the Act. (Three Corners Only) The FTC would also establish an Office to provide business education and guidance. Violation of the Act is an Unfair or Deceptive Act. FTC is given authority over Common Carriers to enforce violations. Cantwell Only gives FTC independent litigation authority. Establishes a Data Victims' Relief Fund		

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL. (a) Civil Action.—In any case in which the attorney general of a State or the chief consumer protection officer of a State has reason to believe that ~~an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an act or practice that violates this~~ Act or a regulation promulgated under this Act, the attorney general of the State, or the chief consumer protection officer of the State, may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State, in an appropriate district court of the United States to— (1) enjoin that act or practice;	SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL. (a) CIVIL ACTION. —In any case in which the attorney general of a State or the chief consumer protection officer of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State, or the chief consumer protection officer of the State, may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State, in an appropriate district court of the United States to— (1) enjoin that act or practice;	SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL. (a) CIVIL ACTION.—In any case in which the attorney general of a State or the chief consumer protection officer of a State has reason to believe that **a covered entity has violated this** Act or a regulation promulgated under this Act**,** the attorney general of the State, or the chief consumer protection officer of the State, may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State, in an appropriate Federal district court of the United States to— (1) enjoin that act or practice;

(2) enforce compliance with this Act or the regulation; (3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State; (4) reasonable attorneys' fees and other litigation costs reasonably incurred; ~~or~~ ~~(5) obtain such other relief as the court may consider to be appropriate.~~	(2) enforce compliance with this Act or the regulation; (3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State; (4) reasonable attorneys' fees and other litigation costs reasonably incurred; or (5) obtain such other relief as the court may consider to be appropriate.	(2) enforce compliance with this Act or the regulation; (3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of the State; **or** (4) reasonable attorneys' fees and other litigation costs reasonably incurred.
(b) Rights of the Commission. —	(b) RIGHTS OF THE COMMISSION. —	(b) RIGHTS OF COMMISSION. —
(1) IN GENERAL. —Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—	(1) IN GENERAL. —Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—	(1) IN GENERAL. —Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—
(A) be heard on all matters arising in such action; and (B) file petitions for appeal of a decision in such action.	(A) be heard on all matters arising in such action; and (B) file petitions for appeal of a decision in such action.	(A) be heard on all matters arising in such action; and (B) file petitions for appeal of a decision in such action.
(2) NOTIFICATION TIMELINE. — Where it is not feasible for the attorney general of a State to provide the notification required by paragraph (1) before initiating a civil action under subsectionm(a), the State shall notify the Commission immediately after initiating the civil action.	(2) NOTIFICATION TIMELINE. — Where it is not feasible for the attorney general of a State to provide the notification required by paragraph (1) before initiating a civil action under subsection (a), the State shall notify the Commission immediately after initiating the civil action.	(2) NOTIFICATION TIMELINE. — Where it is not feasible for the attorney general of a State to provide the notification required by paragraph (1) before initiating a civil action under subsection (a), the State shall notify the Commission immediately after initiating the civil action.
(c) Actions by the Commission.—In any case in which a civil action is instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act, no attorney general or chief consumer protection officer of a State may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under	(c) ACTIONS BY THE COMMISSION. —In any case in which a civil action is instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act, no attorney general or chief consumer protection officer of a State may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under	(c) ACTIONS BY THE COMMISSION.—In any case in which a civil action is instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act, no attorney general or chief consumer protection officer of a State may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under

this Act that is alleged in such complaint. (d) Investigatory Powers. —Nothing in this section shall be construed to prevent the attorney general of a State or the chief consumer protection officer of a State from exercising the powers conferred on the attorney general or the chief consumer protection officer to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence. (e) Venue; Service of Process. — (1) VENUE. —Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code. (2) SERVICE OF PROCESS. —In an action brought under subsection (a), process may be served in any district in which the defendant (A) is an inhabitant; or (B) may be found. (f) Preservation of State Powers. —Except as provided in subsection (c), no provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or the chief consumer protection officer of a State to— (1) bring an action or other regulatory proceeding arising solely under the laws in effect in that State; or (2) exercise the powers conferred on the attorney general or on the chief consumer protection officer of a State by the laws of the State, including the ability to conduct investigations, to	this Act that is alleged in such complaint. (d) INVESTIGATORY POWERS. —Nothing in this section shall be construed to prevent the attorney general of a State or the chief consumer protection officer of a State from exercising the powers conferred on the attorney general or the chief consumer protection officer to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence. (e) VENUE; SERVICE OF PROCESS. — (1) VENUE. —Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code. (2) SERVICE OF PROCESS. —In an action brought under subsection (a), process may be served in any district in which the defendant— (A) is an inhabitant; or (B) may be found. (f) PRESERVATION OF STATE POWERS. —Except as provided in subsection (c), no provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or the chief consumer protection officer of a State to— (1) bring an action or other regulatory proceeding arising solely under the laws in effect in that State; or (2) exercise the powers conferred on the attorney general or on the chief consumer protection officer of a State by the laws of the State, including the	this Act that is alleged in such complaint. (d) INVESTIGATORY POWERS. —Nothing in this section shall be construed to prevent the attorney general of a State or the chief consumer protection officer of a State from exercising the powers conferred on the attorney general or the chief consumer protection officer to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence. (e) VENUE; SERVICE OF PROCESS. — (1) VENUE. —Any action brought under subsection (a) may be brought in an appropriate **Federal** district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code. (2) SERVICE OF PROCESS. —In an action brought under subsection (a), process may be served in any district in which the defendant— (A) is an inhabitant; or (B) may be found. (f) PRESERVATION OF STATE POWERS. —Except as provided in subsection (c), no provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or the chief consumer protection officer of a State to— (1) bring an action or other regulatory proceeding arising solely under the laws in effect in that State; or (2) exercise the powers conferred on the attorney general or on the chief consumer protection officer of a State by the laws of the State, including the

administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.	ability to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.	ability to conduct investigations, administer oaths or affirmations, or compel the attendance of witnesses or the production of documentary or other evidence.
	Notes: Enforcement by State AGs Enables State AGs to bring suit, in which the FTC can intervene.	

Cantwell	**Cantwell Amendment**	**Three Corners**
SEC. 403. ENFORCEMENT BY INDIVIDUALS. (a) Enforcement by Individuals. — (1) IN GENERAL. —Any individual who suffers an injury (including the denial of a right established under this Act) as a result of a violation of this Act or a regulation promulgated under this Act by a covered entity may bring a civil action against such entity in Federal district court. (2) RELIEF. —In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award the plaintiff— (A) an amount equal to the sum of any **actual damages sustained**; (B) injunctive relief; (C) reasonable attorney's fees and litigation costs; **and** **(D) [equitable] or declaratory relief that the court determines just and reasonable.**	**SEC. 403. ENFORCEMENT BY INDIVIDUALS.** (a) ENFORCEMENT BY INDIVIDUALS. — (1) IN GENERAL. —Any individual who suffers an injury (including the denial of a right established under this Act) as a result of a violation of this Act or a regulation promulgated under this Act by a covered entity may bring a civil action against such entity in Federal district court. (2) RELIEF. —In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award the plaintiff— (A) an amount equal to the sum of any actual damages sustained; (B) injunctive relief; **(C) rescission or reformation of contracts;** (D) an order that the covered entity retrieve any covered data shared in violation of this Act; and (E) reasonable attorney's fees and litigation costs.	SEC. 403. ENFORCEMENT BY PERSONS. (a) ENFORCEMENT BY PERSONS. — (1) IN GENERAL. —Beginning 4 years after the date on which this Act takes effect, any person or class of persons who suffers an injury that could be addressed by the relief permitted in paragraph (2) for a violation of this Act or a regulation promulgated under this Act by a covered entity may bring a civil action against such entity in any Federal court of competent jurisdiction. (2) RELIEF. —In a civil action brought under paragraph (1) in which a plaintiff prevails, the court may award the plaintiff— (A) an amount equal to the sum of any **compensatory** damages; (B) injunctive **or declaratory** relief; and (C) reasonable attorney's fees and litigation costs. **(3) RIGHTS OF THE COMMISSION AND STATE ATTORNEYS GENERAL. —** **(A) IN GENERAL. —Prior to a person or class of persons bringing a civil action under paragraph (1),**

		such person or class of persons must first notify the Commission and the attorney general of the State of the persons residence in writing outlining their desire to commence a civil action. Upon receiving such notice, the Commission and State attorney general shall make a determination and respond to such person or class of persons, not later than 60 days after receiving such notice, as to whether they will independently seek to take action, and upon taking action— **(i) be heard on all matters arising in such action; and** **(ii) file petitions for appeal of a decision in such action.** **(B) BAD FAITH. —Any written communication requesting a monetary payment that is sent to a covered entity shall be considered to have been sent in bad faith and shall be unlawful as defined in this Act, if the written communication was sent:** **(i) Prior to the date that is 60 days after either a state attorney general or the Commission has received the notice required under subparagraph (A).** **(ii) After the Commission or attorney general of a State made the determination to independently seek civil actions against such entity as outlined in subparagraph (A).** **(4) FTC STUDY. —Beginning on the date that is 5 years after the date of enactment of this Act, the Commission's Bureau of Economics shall conduct an annual study to determine the economic impacts in the United States of demand letters sent pursuant to this Act and the scope of the rights of a person to bring forth civil actions against covered entities. Such study shall**

		include, but not be limited to include the following: **(A) The impact on increasing insurance rates in the United States.** **(B) The impact on the ability of covered entities to offer new products or services.** **(C) The impact on the creation and growth of startup companies, including tech startup companies.** **(D) Any emerging risks and long-term trends in relevant marketplaces, supply chains., and labor availability.** **(5) REPORT TO CONGRESS. — Not later than 1 year after the first day on which persons and classes of persons are able to bring civil actions under this subsection, and annually thereafter, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that contains the results of the study conducted under paragraph (4).**
(b) Pre-dispute Arbitration Agreements and Pre-dispute Joint Action Waivers Related to Substantial Privacy Harms and Civil Rights Violations. — (1) IN GENERAL—Except as provided in section 303(d), and notwithstanding any other provision of law, at the election of the person alleging conduct constituting a substantial privacy harm or a violation of section 204, or the named representative of a class or in a collective action alleging such conduct, no pre-dispute arbitration agreement or pre-dispute joint-action waiver shall be valid or enforceable with respect to a substantial privacy harm or a violation of section 204.	(b) PRE-DISPUTE ARBITRATION AGREEMENTS. — (1) IN GENERAL. —Except as provided in section 303(d), and notwithstanding any other provision of law, at the election of the person alleging a violation of this Act, no pre-dispute arbitration agreement shall be valid or enforceable with respect to— (A) a claim for a violation involving an individual under the age of 18; (B) a verified claim for a substantial privacy harm; or (C) a claim for injunctive relief to address physical or mental harm as described in section 2(21)(C), provided	(b) PRE-DISPUTE ARBITRATION AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIVERS. — (1) ARBITRATION. — Notwithstanding any other provision of law, no pre-dispute arbitration agreement with respect to an individual under the age of 18 may limit any of the rights provided in this Act.

	that, unless the parties otherwise agree, a claim that seeks monetary damages may proceed with a claim for injunctive relief only if such monetary damages claim satisfies the requirements of subparagraph (B).	
(2) DETERMINATION OF APPLICABILITY. —An issue as to whether this section applies with respect to a dispute shall be determined under Federal law. The applicability of this section to an agreement to arbitrate and the validity and enforceability of an agreement to which this section applies shall be determined by a court, rather than an arbitrator, irrespective of whether the party resisting arbitration challenges the arbitration agreement specifically or in conjunction with other terms of the contract containing such agreement, and irrespective of whether the agreement purports to delegate such determination to an arbitrator.	(2) DETERMINATION OF APPLICABILITY. —Any issue as to whether this section applies to a dispute shall be determined under Federal law. The applicability of this section to an agreement to arbitrate and the validity and enforceability of an agreement to which this section applies shall be determined by a court, rather than an arbitrator, irrespective of whether the party resisting arbitration challenges the arbitration agreement specifically or in conjunction with other terms of the contract containing such agreement, and irrespective of whether the agreement purports to delegate such determination to an arbitrator.	**(2) JOINT ACTION WAIVERS. —** **(A)Notwithstanding any other provision of law, no general agreement for pre-dispute joint action waiver with respect to an individual under the age of 18 may limit any of the rights provided in this Act.** **(B) Notwithstanding any other provision of law, no arbitral or administrative pre-dispute joint action waiver may limit any of the rights provided in this Act irrespective of the age of a party to such an agreement.**
(3) DEFINITIONS. —For purposes of this subsection: (A) PRE-DISPUTE ARBITRATION AGREEMENT. —The term “pre-dispute arbitration agreement” means any agreement to arbitrate a dispute	(3) DEFINITION OF PRE-DISPUTE ARBITRATION AGREEMENT. —For purposes of this subsection, the term ‘‘pre-dispute arbitration	(3) DEFINITIONS. —For purposes of this subsection: (A) PRE-DISPUTE ARBITRATION AGREEMENT. —The term “pre-dispute arbitration agreement” means any agreement to arbitrate a dispute

that has not arisen at the time of the making of the agreement. (B) PRE-DISPUTE JOINT-ACTION WAIVER. —The term "pre-dispute joint-action waiver" means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit or waive the right of 1 of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.	agreement'' means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement. (4) LIMITATIONS. — (A) CLASS ACTIONS. —An individual may seek enforcement pursuant to subsection (a) for a claim alleged in subsection (b)(1), but, absent the agreement of the parties, no representative or class action may be brought under rule 23 of the Federal Rules of Civil Procedure or any other provision of law. (B) CLARIFICATION. —Nothing in subsection (b) shall be construed to limit the enforceability of a pre-dispute arbitration agreement as to any claim other than those permitted pursuant to subsections (b)(1) or (d).	that has not arisen at the time of the making of the agreement. (B) **GENERAL** PRE-DISPUTE JOINT-ACTIONWAIVER.—The term "pre-dispute joint-action waiver" means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit or waive the right of 1 of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other related forum, concerning a dispute that has not yet arisen at the time of the making of the agreement. **(C) ARBITRAL OR ADMINISTRATIVE PRE-DISPUTEJOINT-ACTION WAIVER.—The term "arbitral or administrative pre-dispute joint-action waiver" means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit or waive the right of 1 of the parties to the agreement to participate in a joint, class, or collective action in a arbitral, administrative, or other related forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.**

(c) Right to Cure. — (1) NOTICE. —Subject to paragraph (3), any action under this section may be brought by ~~an individual~~ if, prior to initiating such action **against a covered entity for injunctive relief**, the ~~individual~~ provides to the covered entity **30** days' written notice identifying the specific provisions of this Act the ~~individual~~ alleges have been or are being violated. (2) EFFECT OF CURE. —In the event a cure is possible, if within the ~~30~~ days the covered entity ~~cures~~ the noticed violation and provides the ~~individual~~ an express written statement that the violation has been cured and that no further violations shall occur, an action for injunctive relief may be reasonably dismissed. **[(3) EXCEPTION FOR MONETARY DAMAGES. —No notice shall be required prior to an individual initiating an action solely for actual monetary damages suffered as a result of the alleged violations of this Act.]**	(c) RIGHT TO CURE. — (1) NOTICE. —Subject to paragraph (3), any action under this section may be brought by an individual only if, prior to initiating such action against a covered entity for injunctive relief, the individual provides to the covered entity 30 days' written notice identifying the specific provisions of this Act the individual alleges have been or are being violated. (2) EFFECT OF CURE. —In the event a cure is possible, if within the 30 days the covered entity cures the noticed violation and provides the individual an express written statement that the violation has been cured and that no such further violations shall occur, an action for injunctive relief shall not be permitted. (3) EXCEPTION FOR MONETARY DAMAGES. —No notice shall be required prior to an individual initiating an action solely for actual monetary damages suffered as a result of the alleged violations of this Act. An individual is encouraged to provide notice to the covered entity of the intent to file an action for monetary damages to afford the covered entity an opportunity to expedite a cure. (4) INJUNCTIVE RELIEF FOR A SUBSTANTIAL PRIVACY HARM. —Notice shall not be required under paragraph (1) prior to filing an action for injunctive relief for a substantial privacy harm. An individual who files such an action must serve the defendant not later than 3 business days after filing such action. No such action for injunctive relief for a substantial privacy harm shall be	(c) RIGHT TO CURE. — (1) NOTICE. —Subject to paragraph (3), **with respect to an** action under this section **for (i) injunctive relief; or (ii) an action against a covered entity that meets the requirements of section 209(c) of this Act, such action** may be brought by **a person or class of persons** if—prior to initiating such action—the **person or class or persons** provides to the covered entity **45** days' written notice identifying the specific provisions of this Act the **person or class of persons** alleges have been or are being violated. (2) EFFECT OF CURE**. — Subject to paragraph (3),** in the event a cure is possible, if within the **45** days the covered entity **demonstrates it has cured** the noticed violation **or violations** and provides the **person or class of persons** an express written statement that the violation or violations has been cured and that no further violations shall occur, an action for injunctive relief may be reasonably dismissed.

	dismissed, stayed, or delayed on the grounds that the individual did not provide notice to the covered entity in such time period. An individual is encouraged to provide notice to the covered entity of the intent to file an action for injunctive relief to afford the covered entity an opportunity to expedite a cure.	**(3) RULE OF CONSTRUCTION. — the notice described in paragraph (1) and the reasonable dismissal in paragraph (2) shall not apply more than once to any alleged underlying violation.** **(d) DEMAND LETTER. —If a person or a class of persons sends correspondence to a covered entity alleging a violation of the provisions of this Act and requests a monetary payment, such correspondence shall include the following language: "Please visit the website of the Federal Trade Commission to understand your rights pursuant to this letter" followed by a hyperlink to the webpage of the Commission required under section 201. If such correspondence does not include such language and hyperlink, the person or joint class of persons shall forfeit their rights under this section.**
(d) Applicability. —This section shall only apply to any claim alleging a violation of section 36 101, 201, 202, 203, 204(a), 205, 206(a)(2), 207, or 302.	(d) APPLICABILITY. —This section shall only apply to any claim alleging a violation of section 201, 202, 203, 204(a), 205, 206(a)(2), 207, or 302.	(e) APPLICABILITY. —This section shall only apply to any claim alleging a violation of section 102, 104, 202, 203, 204, 205(a), 205(b), 206(e)(D), 207(a), 208(a), or 302 for which relief under section 403(a)(2) of this Act may be granted.

Notes: Enables Enforcement by Individuals

Cantwell
Establishes private right of action, which comes into force immediately.
Allows recovery of actual damages, injunctive relief, attorney's fees, and equitable relief.
Bars forced arbitration for Substantial Privacy Harms and violations of Civil Rights protections.
Provides 30-day right to cure, except for cases that allege actual monetary damages.

Three Corners
Establishes private right of action, which comes into force 4 years after enactment.
Allows recovery of compensatory damages, injunctive relief, and attorney's fees.

Requires individuals to notify FTC and State AGs before bringing suit. Demands sent to Covered Entities that do not follow this process are considered Bad Faith. Requires FTC study and Report to Congress on the feasibility of ongoing Private Right of Action. Bns arbitration for individuals under 18 years old. Provides 45-day right to cure. Places procedural limitations on serving process to Covered Entities.

PREEMPTION

Cantwell	Cantwell Amendment	Three Corners
SEC. 404. RELATIONSHIP TO FEDERAL AND STATE LAWS. (a) Federal Law Preservation. — (1) IN GENERAL. —Nothing in this Act or a regulation promulgated under this Act shall be construed to limit— (A) the authority of the Commission, or any other Executive agency, under any other provision of law; [(B) any requirement for a common carrier subject to section 64.2011 of title 47, Code of Federal Regulations, regarding information security breaches; or] (C) any other provision of Federal law unless specifically authorized by this Act. (2) APPLICABILITY OF OTHER PRIVACY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), the Family Educational Rights and Privacy Act (20 12 U.S.C. 1232g; part 99 of title 34, Code of Federal Regulations), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C.	SEC. 404. RELATIONSHIP TO FEDERAL AND STATE LAWS. (a) FEDERAL LAW PRESERVATION. — (1) IN GENERAL. —Nothing in this Act or a regulation promulgated under this Act shall be construed to limit— (A) the authority of the Commission, or any other Executive agency, under any other provision of law; (B) any requirement for a common carrier subject to section 64.2011 of title 47, Code of Federal Regulations, regarding information security breaches; or (C) any other provision of Federal law unless specifically authorized by this Act. (2) APPLICABILITY OF OTHER PRIVACY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; part 99 of title 34, Code of Federal Regulations), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C.	SEC. 404. RELATIONSHIP TO FEDERAL AND STATE LAWS. (a) FEDERAL LAW PRESERVATION. — (1) IN GENERAL. —Nothing in this Act or a regulation promulgated under this Act shall be construed to limit— (A) the authority of the Commission, or any other Executive agency, under any other provision of law; (B) any requirement for a common carrier subject to section 64.2011 of title 47, Code of Federal Regulations, regarding information security breaches; or (C) any other provision of Federal law unless specifically authorized by this Act. (2) APPLICABILITY OF OTHER PRIVACY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; part 99 of title 34, Code of Federal Regulations), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C.

1320d–2 note), and is in compliance with the data privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this title, except for **section 205**, with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.	1320d–2 note), and is in compliance with the data privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this title, except for section 205, with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this para15 graph.	1320d–2 note), and is in compliance with the data privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this title, except for **section 208**, **solely and exclusively** with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.
(3) APPLICABILITY OF OTHER DATA SECURITY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), and is in compliance with the information security requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the requirements of **section 205** with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.	(3) APPLICABILITY OF OTHER DATA SECURITY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), and is in compliance with the information security requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the requirements of section 205 with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.	(3) APPLICABILITY OF OTHER DATA SECURITY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), and is in compliance with the information security requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the requirements of **section 208 solely and exclusively** with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.
(b) Preemption of State Laws. —	(b) PREEMPTION OF STATE LAWS. —	(b) PREEMPTION OF STATE LAWS. —
(1) IN GENERAL. —**Except as provided in paragraphs (2) and (3)**, no State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation,	(1) IN GENERAL. —Except as provided in paragraphs (2) and (3), no State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation,	(1) IN GENERAL. —No State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, **or other**

rule, or requirement covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act.	rule, or requirement covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act.	**provision having the force and effect of law of any State, or political subdivision of a State,** covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act.
(2) STATE LAW PRESERVATION.—Paragraph (1) shall not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:	(2) STATE LAW PRESERVATION.—Paragraph (1) shall not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:	(2) STATE LAW PRESERVATION.—Paragraph (1) shall not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:
(A) Consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices.	(A) Consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices.	(A) Consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices. **[**However, the fact of a violation of this Act shall not be pleaded as an element of any violation of such law.**]**
(B) Civil rights laws.	(B) Civil rights laws.	(B) Civil rights laws.
(C) Laws that govern the privacy rights or other protections of employees, employee information, students, or student information.	(C) Laws that govern the privacy rights or other protections of employees, employee information, students, or student information.	(C) Laws that govern the privacy rights or other protections of employees, employee information, students, or student information.
(D) Laws that address notification requirements in the event of a data breach.	(D) Laws that address notification requirements in the event of a data breach.	(D) Laws that address notification requirements in the event of a data breach.
(E) Contract or tort law.	(E) Contract or tort law.	(E) Contract or tort law.
(F) Criminal laws governing fraud, theft, unauthorized access to information or electronic devices, or unauthorized use of information, malicious behavior, or similar provisions, or laws of criminal procedure.	(F) Criminal laws governing fraud, theft, unauthorized access to information or electronic devices, or unauthorized use of information, malicious behavior, or similar provisions, or laws of criminal procedure.	(F) Criminal laws governing fraud, theft, including identity theft, unauthorized access to information or electronic devices, or unauthorized use of information, malicious behavior, or similar provisions, or laws of criminal procedure.
(G) Criminal or civil laws regarding cyberstalking, cyberbullying, nonconsensual pornography, sexual harassment, **or malicious conduct involving the use or misuse of personal information.**	(G) Criminal or civil laws regarding cyberstalking, cyberbullying, nonconsensual pornography, sexual harassment, or malicious con15 duct involving the use or misuse of personal information.	(G) Criminal or civil laws regarding cyberstalking, cyberbullying, nonconsensual pornography, or sexual harassment.
(H) Public safety or sector specific laws unrelated to privacy or security.	(H) Public safety or sector specific laws unrelated to privacy or security.	(H) Public safety or sector specific laws unrelated to privacy or security.
(I) Laws ~~related to~~ public records, criminal justice information systems, arrest records, mug shots, conviction records, or non-conviction records.	(I) Laws related to public records, criminal justice information systems, arrest records, mug shots, conviction records, or non-conviction records.	(I) Laws **that address** public records, criminal justice information systems, arrest records, mug shots, conviction records, or non-conviction records.
(J) Laws related to banking records, financial records, tax records, Social Security numbers, credit cards, identity theft, credit reporting and	(J) Laws related to banking records, financial records, tax records, Social Security numbers, credit cards, identity theft, credit reporting and	(J) Laws that address banking records, financial records, tax records, Social Security numbers, credit cards, credit reporting and investigations, credit

investigations, credit repair, credit clinics, or check-cashing services. (K) Laws ~~related to~~ facial recognition or facial recognition technologies, electronic surveillance, wiretapping, telephone monitoring, ~~tracking, or tracking technologies.~~ (L) ~~Laws related to biometric or genetic information.~~ (M) Laws related to unsolicited email messages, telephone solicitation, or caller ID. (N) Laws ~~related to~~ health information, medical information, medical records, HIV status, or HIV testing. (O) Laws ~~related to~~ the confidentiality of library records. (P) Section 1798.150 of the California Civil Code (as amended on November 3, 2020 by initiative Proposition 24, Section 16). [(3) NONAPPLICATION OF FCC LAWS AND REGULATIONS TO COVERED ENTITIES. — Notwithstanding any other provision of law, any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof or supplementary thereto or any regulation promulgated by the Federal Communications Commission under such Acts shall not apply to any covered entity with respect to the processing or transfer of covered data under this Act.] (c) Preservation of Common Law or Statutory Causes of Action for Civil Relief.—Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law or regulation promulgated under this Act, shall be construed to preempt, displace,	investigations, credit repair, credit clinics, or check-cashing services. (K) Laws related to facial recognition or facial recognition technologies, electronic surveillance, wiretapping, telephone monitoring, tracking, or tracking technologies. (L) Laws related to biometric or genetic information. (M) Laws related to unsolicited email messages, telephone solicitation, or caller ID. (N) Laws related to health information, medical information, medical records, HIV status, or HIV testing. (O) Laws related to the confidentiality of library records. (P) Section 1798.150 of the California Civil Code (as amended on November 3, 2020 by initiative Proposition 24, Section 16). (3) NONAPPLICATION OF FCC LAWS AND REGU20 LATIONS TO COVERED ENTITIES. —Notwithstanding any other provision of law, any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof or supplementary thereto or any regulation promulgated by the Federal Communications Commission under such Acts shall not apply to any covered entity with respect to the processing or transfer of covered data under this Act. (c) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF. — Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law or regulation promulgated under this Act,	repair, credit clinics, or check-cashing services. (K) Laws **that solely address** facial recognition or facial recognition technologies, electronic surveillance, wiretapping, **or** telephone monitoring. (L) **The Biometric Information Privacy Act (740 ICLS 14 etseq.) and the Genetic Information Privacy Act (410 ILCS 513 et seq.).** (M) Laws to address unsolicited email messages, telephone solicitation, or caller ID. (N) Laws **that address** health information, medical information, medical records, HIV status, or HIV testing. (O) Laws **that address** the confidentiality of library records. (P)Section 1798.150 of the California Civil Code (as amended on November 3, 2020, by initiative Proposition 24, Section 16). (3) NONAPPLICATION OF FCC LAWS AND REGULATIONSTO COVERED ENTITIES.— Notwithstanding any other provision of law, any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof or supplementary thereto or any regulation promulgated by the Federal Communications Commission under such Acts shall not apply to any covered entity with respect to the **collecting**, processing, or transfer of covered data under this Act **[insofar as such entity is a satellite carrier, cable operator, or provider of broadband internet access service].** (c) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FORCIVIL RELIEF.— Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law or regulation promulgated under this Act,

or supplant any Federal or State common law rights or remedies, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law, except that the fact of a violation of this Act shall not be pleaded as an element of any such cause of action.	shall be construed to preempt, displace, or supplant any Federal or State common law rights or remedies, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law, except that the fact of a violation of this Act shall not be pleaded as an element of any such cause of action.	shall be construed to preempt, displace, or supplant any Federal or State common law rights or remedies, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law, except that the fact of a violation of this Act shall not be pleaded as an element of any such cause of action.
Notes: Preempts state laws, with exceptions Clarifies that compliance with specific data security requirements constitutes compliance for Covered Data subject to those requirements. Preempts all state statutory law pertaining to privacy except: Consumer protection; civil rights; employee and student privacy; breach notification; contract and torts; criminal laws for identity theft and others; cyberstalking and cyberbullying; public safety and criminal records; banking records; facial recognition; and protection of certain telephone, medical, and library records. Both bills preempt California's privacy laws except for sections on breach. Cantwell preserves all state laws pertaining to biometric and genetic information, while Three Corners only preserves Illinois' laws on the subject (BIPA and GIPA)		