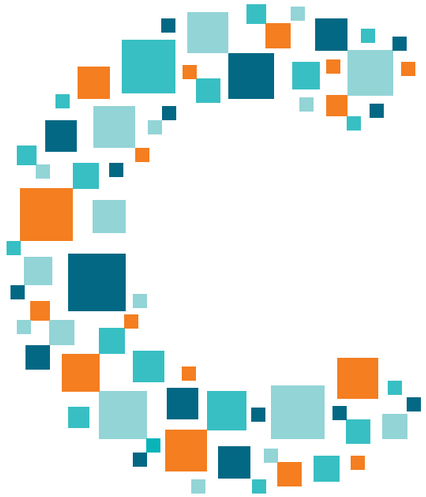
Chamber Technology Engagement Center (C_TEC)

FEDERAL PRIVACY PROPOSALS



_TEC

U.S. Chamber of Commerce
Technology Engagement Center

For more information, please contact:

Jordan Crenshaw | *Policy Counsel*
Chamber Technology Engagement Center
JCrenshaw@uschamber.com

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Definitions	**Covered Entity**	The term "covered entity" — (A) means any organization, corporation, trust, partnership, estate, cooperative, association, sole proprietorship, unincorporated association, or other entity, over which the [FTC] has authority pursuant to section 5(a)(2) of the FTC Act that processes covered information; (B) ...Common Carriers; and (C)...any nonprofit organization...	The term "controller" means a person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information."	(A)The term "covered entity" means a person who (i) intentionally collects, processes, or maintains personal information; and (ii) sends or receives such personal information over the internet or a similar communications network. (B) EXCLUSION.—The term "covered entity" does not include a natural person, except to the extent such person is engaged in a commercial activity that is more than de minimis.	Any natural person who operates in or affects interstate or foreign commerce.	Any entity or person that is subject to the FTC Act and process or transfers covered data. Covered entity includes any entity or person that controls, is controlled by, is under common control with, or shares common branding with a covered entity.
	Covered Information	The term ""covered information""— (i) means any information about an individual possessed by a covered entity that is linked or reasonably linkable to a specific individual **[or consumer device]** and (ii) does not include (I) information that is processed solely for the purpose of employment by the individual's employer, including any information regarding an individual that pertains to such individual in his or her capacity as an owner, director, or employee of a partnership, corporation, trust, estate, cooperative, association, or other type of entity; (II) deidentified information; **[(III) information that is rendered unusable, unreadable, or indecipherable.]**	Sensitive Personal Information and Non-Sensitive Personal Information	(A) The term "personal information" means any information maintained by a covered entity that is linked or reasonably linkable to a specific individual or a specific device, including de-identified personal information and the means to behavioral personalization created or linked to a "specific" individual. (B) EXCLUSIONS.—The term "personal information" does not include (i) publicly available information related to an individual or (ii) information derived or inferred from personal information, if the derived or inferred information is not linked or reasonably linkable to a specific individual.	• The term "covered data" means information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual. • Excluded are aggregated data, de-identified data; employee data; and publicly available data.	"Covered Data" means information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data. Excluded are de-identified data, employee data, and public records.
	Sensitive Information		(A) The term "sensitive personal information" means information relating to an identified or identifiable individual, including the following: i. Financial account information. ii. Health information. iii. Genetic data. iv. Information pertaining to children under 13 years of age. v. Social Security numbers. vi. Unique government-issued identifiers. vii. Authentication credentials, such as a username and password. viii. Precise geolocation information. ix. Content of a wire communication, oral communication, or electronic communications with respect to any entity that is not the intended recipient of the communication. x. Call detail records. xi. Web browsing history, application usage history, and the functional equivalent of either. xii. Biometric information. xiii. Sexual orientation. xiv. Religious beliefs. (B) The term "sensitive personal information" does not include (I) de-identified information...(ii) information related to employment; or (iii) publicly available information.	No	• Covered data that describes or reveals the diagnosis or treatment of past, present, or future physical health, mental health, or disability of an individual. • A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account. • Biometric information. • Contents of Private Communications • Account log-in credentials such as user name or email address, in combination with password or security questions to would permit access. • Covered data revealing racial or ethnic origin, or a religion in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information. • Covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information. • Online activities related to sensitive information defined by the Act. • Calendar, address book, phone or text logs, photos or vides on an individual's device. • Categories designated in rulemaking by FTC.	"Sensitive Covered Data" means the following forms of covered data: • A government-issued identifier, such as a Social Security number, passport number, or driver's license number. • Any information that describes or reveals the past, present, or future physical health, mental health, disability, or diagnosis of an individual. • A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account. • Biometric information. • Precise geolocation information that that reveals the past or present actual physical location of an individual or device. • The content or metadata of an individual's private communications. • An email address, telephone number, or account log-in credentials. • Information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation regarding disclosure. • Information revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure. • Information revealing online activities over time and across third-party website or online services. • Calendar, address book, phone or text logs, photos, or videos maintained on an individual's device. • A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual. • Any other covered data process or transferred for the purpose of identifying sensitive data defined by Act. • Information determined by FTC rulemaking to be sensitive.

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Obligations, Consumer Rights and Prohibitions	**Transparency**	Yes	Yes	Yes	Yes	Yes
	Access	Yes	No	Yes (Categories of Personal Information and Content of Communications)	Yes	Yes
	Correction	Yes	No	Yes	Yes	Yes
	Deletion	Yes	No	Yes	Yes	Yes
	Portability	No	No	Yes	Yes	Yes
	Fiduciary Duty	No	No	No	No	Yes
	AI Specific or Right to Human Review of Automated Decision Making	No	No	Right to Human Review	Study	Required Impact Assessment for algorithmic decision-making for housing, education, employment or credit.
	Reasonable Basis	No	No	Required for collection, processing, disclosure and maintenance of personal information	No	No
	Opt-In	Data Processing Not Consistent with Reasonable Expectations	Any functionality that involves the collection, storage, processing, sale, sharing, or other use of sensitive personal information	• Behavioral Personalization • Data Retention • Disclosure or Sale • Collection, Processing, Maintenance, and Disclosure personal information that creates or increases the risk of foreseeable privacy harms	Processing of and Transferring of Sensitive Covered Data to Third Party	Processing and Transfer of Sensitive Covered Data
	Opt Out	First Party Marketing	Any collection, storage, processing, selling, sharing, or other use of non-sensitive personal information	No	No	Transfer of Data to Third Parties

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Obligations, Consumer Rights and Prohibitions *(continued)*	**Misc. Prohibited Practices**	• Collection Under False Pretenses • Processing of Biometrics • Processing of Attribution of Devices to Individuals with Probabilistic Methods • Processing of Covered Information obtained through microphone or camera • Processing of Contents of Communications • Processing of Health Information	No	• Disclosing Personal Information with intent to threaten, intimidate, or harass any person, incite or facilitate the commission of a crime of violence, or place any person in reasonable fear of death or serious bodily injury • Disclosure to entities not subject to United States jurisdiction or not Compliant with the Act • Reidentifying personal information • Deceptive Notice and Consent Processes and Privacy Policies • Collection, Processing, Maintenance, or Disclosure of Genetic Information subject to exceptions • Collection, Processing, and Disclosure of Contents of Communications	No	No
	Data Minimization	No longer than reasonably necessary for purposes information originally processed	No	• A covered entity shall not maintain personal information for more time than expressly consented to by an individual whose personal information is being maintained • Covered entities may not collect, process, disclose, or maintain personal information for more than reasonably necessary	Entities Shall not Collect, Process, or Transfer covered data beyond what is reasonably necessary, proportionate, and limited to provide or improve a produce, service or a communication about a product or service, including what is reasonably necessary, proportionate and limited to provide a product or service specifically requested by an individual or reasonably anticipated within the context of the covered entity's ongoing relationship with an individual; OR What is reasonably necessary, proportionate, or limited to otherwise process or transfer covered data in a manner that is described in the required privacy policy	A covered entity shall not process or transfer covered data beyond what is reasonably necessary, proportionate and limited to specific processing purposes and transfers described in required privacy policy, where the covered entity has affirmative express consent or explicitly excepted by the Act
	Discrimination	Race, color, religion, national origin, sex, age or disability	No	No processing of personal information or contents of communication for advertising, marketing soliciting, offering, selling, leasing, licensing, renting or otherwise commercially contracting for employment, finance, health, credit, insurance, house, or education opportunities that discriminates against a protected class.	No	A covered entity shall not process or transfer covered data on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income or disability for advertising, marketing, soliciting, offering, selling, leasing, licensing, renting or commercially contract for housing, employment, credit, or education opportunity in a manner that unlawfully discriminates or segregates or discriminates place of public accommodation

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Obligations, Consumer Rights and Prohibitions *(continued)*	**Pricing and Service Differences**	Prohibition on Take-It-Or-Leave it and Financial Incentives	No	No	Covered entities may not deny goods or services because of the exercising of privacy rights	Generally, Covered entities cannot condition provision of service or product to an individual on the individual's agreement to waive privacy rights with some exceptions
Accountability	**Privacy Program**	Yes	No	No	Yes	Yes
	Audit Requirement	No	Yes	No	Required Privacy Impact Assessment	No
	Privacy/ Security Officer Requirement	Both	No	No	Both	Both
Security	**Data Security**	Requires reasonable administrative, technical and physical security measures, polices, practices and procedures.	No	• Covered entities must establish and implement reasonable information security policies, practices, and procedures for the protection of personal information collected, processed, maintained, or disclosed. • Must notify Agency within 72 hours of awareness of data breach or data sharing abuse.	Covered entities must establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risk to the confidentiality, security, and integrity of sensitive covered data	A covered entity shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data. Such data security practices shall be appropriate to the volume and nature of the covered data at issues. Practices should include a vulnerabilities assessments, information retention and disposal, and training
Misc. Industries	**Service Providers and Processors**	Covered entities may only disclose covered information to processors with a written agreement limiting processing	Service Provider with contract limiting processing not considered a third party	Service providers are not third parties if they have a contract limiting processing, do not directly collect personal information, and only derive revenue form processing for covered entities, do not disclose personal information to third parties, do not provide targeting, and do not link information from covered entity to another source.	• Service Providers are Not Third Parties • Service providers are exempt from access, deletion, correction, and portability rights.	• Service Providers are not third parties so long as their processing or transferal relates to the performance of service on behalf or direction of covered entity. • Service Providers are exempt from access, transparency, deletion, correction and individual control rights.
	Data Brokers	Public identification as data broker, auditing, and FTC registry	No	No	Registration with FTC	No

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Misc. Industries *(continued)*	**Small Business Relief**	Small businesses that have an **[annual gross revenue or less]**, process covered information of fewer than **[50,000]** individuals, **[and derives less than 50 percent of its annual revenues from selling consumers' personal information]** alone or in a group may apply to the FTC for self-regulatory safe harbors.	Audit exemption of controllers who collect, store, process, sell, share, or otherwise use sensitive personal information relation to 5,000 or fewer individuals	Small businesses are defined as covered entities that do not earn revenue from the sale of personal information; earn less than half of annual revenues from the processing of personal information; have not maintained over the last six month personal information of over 250,000 individuals; have fewer than 200 employees; and receive less than $25M in annual revenue. Small businesses are exempted from access, correction, portability requirements and can follow approved safe harbor programs for larger companies.	Small businesses that in the previous three years did not exceed a gross revenue of $25M, or process covered data of 100,000 more individuals or devices, or derive 50 percent or more of their revenues from data sales are exempted from access, correction, deletion, minimization, and portability rights.	Small businesses which over the past three calendar years that do not maintain annual average gross revenues exceeding $25M, annually process the covered data of an average of 100,000 or more individuals, h households or devices; AND derive 50 percent or more of their annual revenue from transferring individuals' covered data are exempted from the Act.
	Children's Privacy	**Bracketed**	Information pertaining to children under 13 considered sensitive personal information	No	No	No
Enforcement Issues and Effective Date	**Enforcement Agency**	FTC with new Bureau of Privacy	FTC with additional 50 full-time staff and $35M in appropriations	United States Digital Privacy Agency led by appointed Director	FTC	FTC with new privacy bureau
	Safe Harbor	See Small Business Relief	No	• Safe harbor program for disclosing personal information to entities outside United States jurisdiction • Disclosure of Contents of Communications for Service Providers • Genetic Information Processing and Disclosure for Service Providers • Agency-approved "notice and consent" safe harbor	FTC-approved certification programs create deemed compliance	
	Expanded Penalty Authority	Civil Penalties	No	• Criminal penalties for disclosure with intent to harm (fine or 5 years in prison) • Civil Penalties with Maximums • Rescission or Reformation of Contracts • Refund of Moneys • Restitution • Disgorgement • Damages • Limits on Activities • Public Notice of Violations	No	No
	State AG Enforcement	Yes	Yes	Yes	Yes	Yes
	Rulemaking	Yes	Yes	Yes	Yes	Yes

		Energy and Commerce ("_____ Act of 2019")	H.R. 2013 (Delbene, "Information Transparency & Personal Data Control Act")	H.R. 4978 (Eshoo, "Online Privacy Act of 2019.")	Wicker, "United States Consumer Data Privacy Act of 2019."	S. 2968 (Cantwell, "Consumer Online Privacy Rights Act")
Enforcement Issues and Effective Date *(continued)*	**Private Right of Action**	**Bracketed**	No	Injunctive Relief and Damages	No	Yes
	Effective Date	**Bracketed**	180 days after enactment	1 year after enactment	2 years after enactment	180 days after enactment
	Preemption	**Bracketed**	For a controller that is subject to this Act, or any regulation promulgated pursuant to this Act, the provisions of this Act, or any such regulation, shall preempt any civil provision of the law of any State or political subdivision of a State to the degree the law is focused on the reduction of privacy risk through the regulation of the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.	No	No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or security and associated activity of covered entities.	(c) Preemption of directly conflicting State laws.—Except as provided in subsections (b) and (d), this Act shall supersede any State law to the extent such law directly conflicts with the provisions of this Act, or a standard, rule, or regulation promulgated under this Act, and then only to the extent of such direct conflict. Any State law, rule, or regulation shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under this Act.

U.S. Chamber of Commerce
Technology Engagement Center

Chamber Technology Engagement Center (C_TEC)

FEDERAL PRIVACY PROPOSALS

For more information, please contact:

Jordan Crenshaw | *Policy Counsel*
Chamber Technology Engagement Center
JCrenshaw@uschamber.com