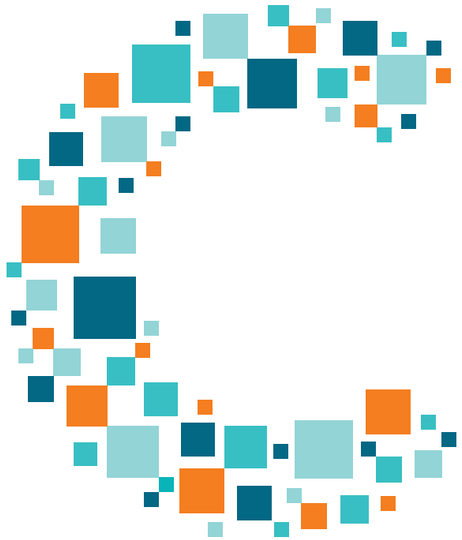
REPUBLICAN

FEDERAL PRIVACY PROPOSALS



_TEC

U.S. Chamber of Commerce
Technology Engagement Center

For more information, please contact:

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

		Energy and Commerce ("_____ Act of 2019")	S. 3456, (Moran, "Consumer Data Privacy and Security Act of 2020")	S___, (Wicker, “Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act” or “SAFE 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...	Any entity that— (i) alone, or jointly with others, determines the purpose and means of collecting or processing personal data; and (ii) is—under FTC Act Section 5(2)(a) authority, common carrier under the 1934 Communications Act, or non-profit organizations	Any person that— (A) is subject to the FTC Act or common carrier described in 15 U.S.C. 45(a)(2), or not profits; (B) collects, processes, or transfers covered data; AND (C) determines the purposes and means of such collection, processing, or transfer.
	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) de-identified information; **[(III) information that is rendered unusable, unreadable, or indecipherable.]**	"Personal data" means information that identifies or is linked or reasonably linkable to a specific individual. "Linked or reasonably linkable" means data that can be used on its own or in combination with other information held by, or readily accessible to, the covered entity or service provider to identify the individual. This includes persistent identifiers like IP addresses, serial numbers, cookies, and unique device identifiers. Excluded are de-identified data, unreadable or undecipherable data, employee data, publicly available data, or pseudonymous data.	• The term "covered data" means information that identifies or is linked ore 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.
	Sensitive Information		"Personal data" that is: • A unique, government-issued identifier, such as a social security number, passport number, driver's license number, or a taxpayer identification number • A username or email address in combination with a password or security question and answer that would permit access to an online account • Biometric information • Content of a wire communication, oral communication, or electronic communication defined in 18 U.S.C. 2510 • Info that relates to the past, present, or future diagnosed physical or mental health or condition of an individual; the provision of heath care to an individual; or the past, present, or future payment for the provision of health care to an individual • Financial account number, debit card number, credit card number, if combined with an access code, password, or credentials that provide access to such an account • Religious beliefs or affiliation • Sexual orientation • Precise geolocation • Data determined by FTC Rulemaking	Covered that is: • A unique, government-issued identifier, such as a Social Security number, passport number, or driver’s license number, that is not required to be displayed to the public • Any covered data that describes or reveals that diagnosis or treatment of the 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 access code, password, or credentials allowing access to any such account • Biometric Information • A persistent identifier • Precise geolocation information • The contents of an individual’s private communications, such as emails, texts, direct messages, or mail, or the identity of the parties subject to such communications, unless the covered entity is the intended recipient of the communication • Account log-in credentials such as a user name or email address, in combination with a password or security question and answer that would permit access to an online account • Covered data revealing an individual’s racial or ethnic origin, or 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 • Covered data about the online activities of an individual that addresses or reveals a category of covered data described in another subparagraph of this paragraph • Covered data that is calendar information, address book information, phone or text logs, photos, or videos maintained for private use on an individual’s device • Any covered data collected or processed by a covered data for the purpose of identifying covered data described in another paragraph of this paragraph • Any other category of covered data designated by FTC rulemaking

		Energy and Commerce ("_____ Act of 2019")	S. 3456, (Moran, "Consumer Data Privacy and Security Act of 2020")	S___, (Wicker, “Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act” or “SAFE Act”)
Obligations, Consumer Rights and Prohibitions	**Transparency**	Yes	Yes	Yes
	Access	Yes	Yes	Yes
	Correction	Yes	Yes	Yes
	Deletion	Yes	Yes	Yes
	Portability	No	Yes	Yes
	Fiduciary Duty	No	No	No
	AI Specific or Right to Human Review of Automated Decision Making	No	No	• A.I. Transparency Reports Required • Filter Bubble Transparency Act (requiring option for filter-less search) • Informed consent of practices relating to "manipulation" of user interfaces for large online operators
	Reasonable Basis	No	Yes	No
	Opt-In	Data Processing Not Consistent with Reasonable Expectations	Processing of personal data without consent or permissible purpose. Not required of third parties if notice provide by first-party company. Consent can be inferred. Affirmative express consent required for processing of sensitive personal data	Processing of and Transferring of Sensitive Covered Data to Third Party
	Opt Out	First Party Marketing	N/A	No

		Energy and Commerce ("_____ Act of 2019")	S. 3456, (Moran, "Consumer Data Privacy and Security Act of 2020")	S___, (Wicker, “Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act” or “SAFE 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	N/A	Filter Bubble and DETOURS Act (see AI section)
	Data Minimization	No longer than reasonably necessary for purposes information originally processed	Must conduct impact assessments for material changes in processing	Covered entities shall not collect, process, or transfer data beyond-- (1) what is reasonably necessary, proportionated, and limited to provide or improve a product, service, or a communication about a product or service, including what is reasonably necessary, proportionated, 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; (2) what is reasonably necessary, proportionated, or limited to otherwise process or transfer covered data in a manner that is described in the privacy policy that the covered entity is required to publish under the Act; (2) what is expressly permitted by this Act or federal law. The FTC is required within one year to develop best practices for minimization.
	Discrimination	Race, color, religion, national origin, sex, age or disability	No	No
	Pricing and Service Differences	Prohibition on Take-It-Or-Leave it and Financial Incentives	No	No denial of products or services to an individual because individual has exercised access, correction, or portability rights
Accountability	**Privacy Program**	Yes	Yes	Yes
	Audit Requirement	No	Large data holders required to have privacy impact assessment	Large data holders required to have privacy impact assessments
	Privacy/ Security Officer Requirement	Both	Both	Both

		Energy and Commerce ("_____ Act of 2019")	S. 3456, (Moran, "Consumer Data Privacy and Security Act of 2020")	S___, (Wicker, “Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act” or “SAFE Act”)
Security	**Data Security**	Requires reasonable administrative, technical and physical security measures, polices, practices and procedures.	Covered entities and service providers shall develop, document, implement, and maintain a comprehensive data security program that contains reasonable administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity or personal data from unauthorized access, use, destruction, acquisition, modification, or disclosure.	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 covered data.
Misc. Industries	**Service Providers and Processors**	Covered entities may only disclose covered information to processors with a written agreement limiting processing	Covered entities shall only disclose personal data to a service provider pursuant to a contract that is binding on both parties and meets the following requirements: service providers only collect or process personal data as directed by covered entity; establish purposes for collecting and processing personal data, and a reasonable representation from service provider establishing appropriate procedures and controls. • Controllers required to have due diligence of service providers • Service providers required to assist covered entities as practicable for control requests • Service providers required to delete data after performance • Service providers required to provide written representation of compliance	• Service providers shall not process service provider data for any processing purpose not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider; shall not transfer service provider data to a third party for any purpose other than a purpose performed on behalf of, or at the direction of, the covered entity that transferred the data to the service provider without the affirmative express consent of the individual to whom the service provider data relates. • Service providers required to delete or deidentify service provider data as practicable after completion of service or service period. • Service providers exempted from access, correction, portability, deletion requirements but shall help covered entity comply as practicable upon receiving notice from the covered entity. • Service providers are exempted from opt-in for sensitive data and covered entity data minimization requirements. • Due diligence required by covered entities for service providers FTC required to provide guidance within 2 years for service provider relationship issues.
	Data Brokers	Public identification as data broker, auditing, and FTC registry	No	Registration with FTC
	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.	Accuracy, Correction, and Access requests not required for small businesses and compliance for other misc. requirements takes into whether a small business. A small business is a covered entity or service provider that in the last six months did not employ more than 500 employees and did not maintain $50 million or more in average gross receipts over the last three years. Additionally to be considered a small business, an entity cannot collect or process annually the personal data of 1 million or more individuals OR the sensitive personal data of 100,000 or more individuals.	Covered entities noted required to comply with access, correction, deletion, and portability requests, data minimization requirements or have privacy/security officers if— (1) the covered entity's average annual gross revenues did not exceed $50 million (2) on average, the covered entity annual processed the covered data of less than 1 million individuals; (3) the covered entity never employed more than 500 individuals at any one time; AND (4) the covered entity derived less than 50 percent of its revenues from transferring covered data.
	Children's Privacy	**Bracketed**	No	No

		Energy and Commerce ("_____ Act of 2019")	S. 3456, (Moran, "Consumer Data Privacy and Security Act of 2020")	S___, (Wicker, “Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act” or “SAFE Act”)
Enforcement Issues and Effective Date	**Enforcement Agency**	FTC with new Bureau of Privacy	FTC	FTC (also expands authority under 13(B))
	Safe Harbor	See Small Business Relief		FTC-approved certification programs enabled deemed compliance
	Expanded Penalty Authority	Civil Penalties	Civil Penalty	No
	State AG Enforcement	Yes	Yes	Yes
	Rulemaking	Yes	Yes	Yes
	Private Right of Action	**Bracketed**	No	No
	Effective Date	**Bracketed**	1 year after enactment but preemption kicks in immediately.	18 months after enactment
	Preemption	**Bracketed**	The Act shall supersede any provision of a law, rule, regulation, or other requirement of any State or political subdivision of a State to the extent that such provision relates to the privacy or security of personal data except for data breach, general standards of fraud and public safety, student privacy, GLBA entities, HIPAA entities, and employment, and discrimination.	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.