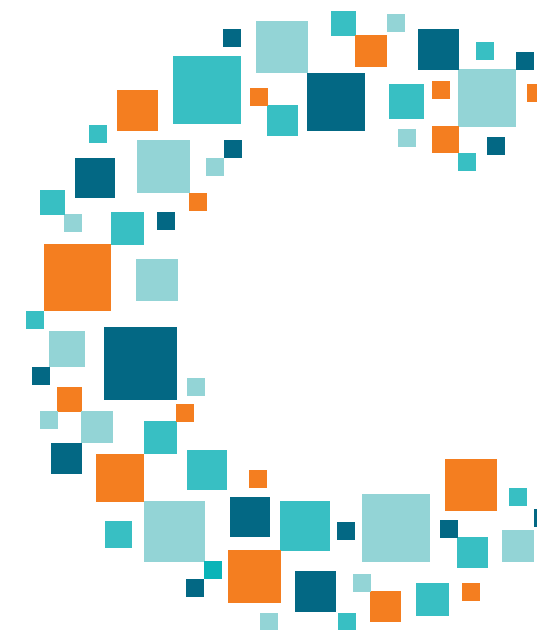


Chamber Technology Engagement Center (C_TEC)

COVID-19 PRIVACY BILL COMPARISON



_TEC

U.S. Chamber of Commerce
Technology Engagement Center

For more information, please contact:

**Jordan
Crenshaw**

*Executive Director and Policy Counsel
Chamber Technology Engagement Center
JCrenshaw@uschamber.com*

		Democratic Plan (Public Health Emergency Privacy Act)	Republican Plan (COVID-19 Consumer Data Protection Act of 2020)	Cantwell/Cassidy
Definitions	Covered Entity	<p>Any person (including government entity)-(i) that collects, uses or discloses emergency health data electronically or through communications by wire or radio; OR (ii) that develops or operates a website, web application, mobile application, mobile operating system feature, or smart device application for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency.</p> <p>EXCLUSIONS- (i) health care providers, (ii) de minimis collection or processing of emergency health data; (iii) service provider; (iv) a person acting in their individual or household capacity; or (v) a public health authority, (vi) HIPAA covered entities or business associates.</p>	<p>With respect to covered data, any entity or person that is (i) subject to FTC enforcement; or a (ii) common carrier or nonprofit organization that collects, processes, or transfers such data, or determines the means and purposes for the collection, processing, or transfer of covered data; and is not a service provider with respect to such data.</p>	<p>Operators of “automated exposure notification services” other than public health authority that are subject to the FTC Act, non profits or common carriers.</p> <p>An “automated exposure notification service” is a website, online service, online application, mobile application, or mobile operating system that is offered in commerce in the United States and that is designed, in part or in full, specifically to be used for, or marketed for, the purpose of digitally notifying in an automated manner, an individual who may have become exposed to infectious disease (or the device of such individual, or a personal or entity that reviews such disclosures).</p>
	Emergency Health Data/Covered Data	<p>Means data linked or reasonably linkable to an individual or device, including data inferred or derived about the individual or device from other collected data provided such data is still linked or reasonably linkable to the individual or device, that concerns the public COVID-19 health emergency. Such data includes-</p> <p>(A) information that reveals the past, present, or future physical or behavioral health or condition of, or provision of healthcare to, an individual, including-</p> <ul style="list-style-type: none"> (i) data derived from the testing or examination of a body part or bodily substance, or a request for such testing; (ii) whether or not an individual contracted or been tested for, or an estimate of the likelihood that a particular individual may contract, such disease or disorder; and (iii) genetic data, biological samples, and biometrics; and <p>(B) other data collected in conjunction with other emergency health data or for the purpose of tracking, screening, monitoring, contact tracing, or mitigation, or otherwise responding to the COVID-19 public health emergency, including-</p> <ul style="list-style-type: none"> (i) geolocation data, when such term means data capable of determining the past or present precise physical location of an individual at a specific point in time, taking account of population densities, including cell-site location information, triangulation data derived from nearby wireless or radio frequency networks, and global positioning system data; (ii) proximity data, when such term means information that identifies or estimates the past or present physical proximity of one individual or device to an another, including information derived from Bluetooth, audio signatures, nearby wireless networks, and near-field communications; (iii) demographic data; (iv) contact information for identifiable individuals or a history of the individual's contacts over a period of time, such as an address book or call log; and (v) any other data collected from a personal device. 	<p>Precise geolocation data, proximity data, a persistent identifier, and personal health information to track the spread signs or symptoms of COVID-19, to measure compliance with social distancing or other COVID-19 requirements, or for contact tracing.</p> <p>EXCLUSIONS-</p> <ul style="list-style-type: none"> (i) Aggregated data (ii) Business contact information (iii) De-identified data (iv) Employee screening data (v) Publicly available information 	<p>Any information that is 1) linked or reasonably linkable to any individual or device linked or reasonably linkable to an individual; 2) not aggregate data; and 3) collected, processed, or transferred in connection with an automated exposure notification service.</p>
Requirements	Purpose Limitation	Yes	Yes	Yes
	Accuracy Requirement	Yes	Yes	Yes

		Democratic Plan (Public Health Emergency Privacy Act)	Republican Plan (COVID-19 Consumer Data Protection Act of 2020)	Cantwell/Cassidy
Requirements <i>(continued)</i>	Safeguards Against Discrimination	Yes	No	Yes
	Limitations on Disclosures to Government Entities	Yes	No	Yes
	Security Standards	Yes	Yes	Yes
	Other Prohibitions	(i) Commercial advertising (ii) Discrimination in employment, finance, credit, insurance, housing, or education opportunities (iii) Segregating, discriminating in, or otherwise making unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation (iv) Denial of right to vote (v) Pre-dispute arbitration	No	(i) Collection, processing, or transferring an actual, potential, or presumptive positive diagnosis of an infectious disease as part of the automated exposure notification service, unless an it is an authorized diagnosis confirmed by a public health authority or a licensed healthcare provider. (ii) Required collaboration with public health authorities (iii) Collection or processing for commercial purposes. (iv) Transferring data except for notification for enrolled individuals, public health authorities, and service provider with certain contract provisions, or to comply with establishment, exercise, or defense of a legal claim.
	Opt-In	Collection, use, or disclosure of emergency health data. EXCEPTIONS– (i) protecting against malicious, deceptive, fraudulent, or illegal activity; (ii) detecting, responding to, or preventing information security incidents or threats; OR the covered organization is compelled to do so by legal obligation.	Collection, processing, sharing of covered data	Enrollment in automated exposure notification system
	Revocation of Consent	Allowed and companies required to cease collection, use, and disclosure no later than 15 days and must destroy data 30 days after revocation.	Yes and covered entity must cease within 14 days collection, processing, and disclosure.	Yes
	Notice Requirement	Yes	Yes	Yes
	Reporting Requirement	Every 90 days if collects, uses, or processes data about 100,000 or more individuals	30 days after enactment and not fewer than every 60 days after.	No
	Data Minimization	Destroyed emergency health information 60 days after termination of public health emergency.	(i) May not collect covered data beyond COVID-19 purposes. (ii) Deletion required of covered data when data no longer used for COVID-19 purpose and no longer necessary to comply with laws.	No
	Right to Delete	No	No	Yes
General Exceptions	Other General Exceptions	(i) manual contact tracing (ii) public health and research for nonprofits OR vaccine or drug research	Comply with legal obligation	Research

		Democratic Plan (Public Health Emergency Privacy Act)	Republican Plan (COVID-19 Consumer Data Protection Act of 2020)	Cantwell/Cassidy
Enforcement and Preemption	FTC Enforcement	Yes	Yes	Yes
	FTC Rulemaking	Yes	No	No
	State AG Enforcement	Yes	Yes	Yes
	Private Right of Action	(i) Damages of \$100 to \$1,000 for negligence (ii) \$500 to \$5,000 for reckless, willful or intentional violations (iii) attorneys fees (iv) injunctive relief	No	No
	Preemption	No	Yes (not definitive if complete)	No
	Effective Date	30 days after enactment	Not enumerated	Date of Enactment