Comprehensive Federal Privacy Legislation Can Build on State Privacy Laws

The United States needs a strong, comprehensive federal privacy law that ensures consumers' personal data is used in ways they expect.

Congress should build on privacy laws enacted by California and Virginia to create comprehensive federal legislation that protects consumers nationwide. A new federal privacy law should not only contain the rights and protections included in these state privacy laws but should create new rights and obligations that ensure businesses are accountable for handling personal data in line with consumers' expectations.

There are three key components of privacy legislation: (1) establishing consumers' rights in their data, (2) obligating companies to handle that data in ways that do not surprise consumers, and (3) strong enforcement. **Congress should enact a federal law that builds on these state privacy protections in each area.**

CONSUMER RIGHTS

California (CCPA + CPRA)	Virginia (CDPA)	Federal Privacy Law
California creates new consumer rights including:	Virginia creates new consumer rights including:	A new federal privacy law should create rights for consumers, including:
✔ Confirmation of Processing	✔ Confirmation of Processing	Confirmation of Processing
✔ Access	✔ Access	Access
✔ Correction	✔ Correction	Correction
✔ Deletion	✔ Deletion	Deletion
✔ Portability	✔ Portability	Portability
✔ Opt out rights: from sale and "sharing" of personal information	✔ Opt out rights: from sale, targeted advertising, and certain types of "profiling"	Consumers should have broad rights to opt out of processing—not just sale

OBLIGATIONS ON COMPANIES

For companies that decide how and why consumers' data is collected or used:

California (CCPA + CPRA)	Virginia (CDPA)	Federal Privacy Law
California imposes several obligations on businesses, including:	Virginia imposes a broad set of obligations on businesses, including:	A new federal privacy law can impose a broad range of obligations on businesses to use data in line with consumers' expectations, including:
✔ Data minimization and purpose specification	✔ Data minimization and purpose specification	Data minimization and purpose specification
✖ For sensitive data, consumers have the burden to opt out of certain uses	✔ For sensitive data, controllers have the burden to obtain consumer's consent	For sensitive data, controllers should have the burden to obtain consumers' consent
✖ Consent is only required in narrow circumstances: (1) selling or sharing personal information of minors, (2) offering financial incentives	✔ Consent is not required for uses consumers expect, but is required for: (1) unexpected uses, (2) processing of sensitive personal data	Requiring consent for unexpected or sensitive uses, but not for uses that consumers expect
✔ Reasonable security measures required	✔ Reasonable security measures required	Reasonable security measures

For companies that decide how and why consumers' data is collected or used *(continued)*:		
California (CCPA + CPRA)	**Virginia (CDPA)**	**Federal Privacy Law**
✔ Future regulations are to require risk assessments for activities that present "significant risks"	✔ Data protection assessments are required for specific activities, including targeted advertising, sale of data, and processing of sensitive personal data	Data protection assessments that require companies to assess activities that may create heightened concerns
✔ Prohibition on retaliating against consumers who exercise new rights	✔ Prohibition on retaliating against consumers who exercise new rights	Prohibit retaliation against consumers who exercise new rights
✖ Non-discrimination is not addressed	✔ Prohibition on processing personal data in violation of state and federal non-discrimination laws	Prohibit processing data in violation of non-discrimination laws
For companies acting as service providers or data processors:		
California recognizes the distinct role of service providers in protecting the privacy of consumers' personal information	**Virginia recognizes the distinct role of processors in protecting the privacy of consumers' personal information**	**A new federal privacy law can recognize the distinct role of processors in protecting the privacy of consumers' personal information, including by:**
✔ Contract required; service providers must process data on behalf of businesses and pursuant to a contract	✔ Contract required; processors must process data on behalf of controllers and pursuant to a contract	Requiring contracts between controllers and processors, to ensure that processors act on behalf of controllers
✖ Data security obligations are not specifically applied to service providers	✔ Data security obligations apply to processors in addition to controllers	Applying data security obligations to processors in addition to controllers
✔ For consumer rights requests, service providers are not required to respond directly to consumer requests but are to provide assistance to businesses	✔ For consumer rights requests, processors not required to respond directly to consumer requests but are to provide assistance to controllers	For consumer rights requests, requiring processors to provide assistance to controllers, but not requiring processors to respond directly to consumer requests
✔ Subcontractors must be engaged via written contracts that pass on the service provider's obligations under the law	✔ Subcontractors must be engaged via written contracts that pass on the processor's obligations under the law	Requiring subcontractors be engaged via written contracts that pass on the processor's obligations under the law
✖ Does not address duty of confidentiality	✔ Duty of confidentiality must be imposed by processors on persons who process data	Require a duty of confidentiality be placed on persons who process data
✖ Does not address treatment of data after end of services	✔ At the end of services, data must be deleted or returned to the controller	After the end of services, require a processor to either delete, de-identify, or return data to a controller, as set out in their contract
✔ Contract is to specify a business's right to take "reasonable and appropriate steps" to ensure service provider uses personal information consistent with obligations	✔ Requires processors to either arrange an assessment and provide it to a controller upon request or cooperate with "reasonable assessments" by a controller	Require processors to either arrange for assessments and provide them to controllers upon request or cooperate with a controller's reasonable assessment
ENFORCEMENT		
The privacy provisions of California's law are to be enforced by a new regulator, the California Privacy Protection Agency	Virginia's Attorney General is to enforce the statute	A federal privacy law should not be enforced by a single regulator, but by federal and state agencies working together **Federal:** The FTC should enforce federal privacy law, with new tools including: 1. Targeted rulemaking authority 2. Authority to fine first-time violators 3. Additional funding and staff **State:** Attorneys General in all states and territories should also enforce the law, adding 50+ new enforcement agencies

✔ Addressed ⁘ Partially Addressed ✖ Not Addressed