A Framework for Federal Privacy Legislation

The Insights Association supports a comprehensive federal consumer data privacy law that will respect and protect consumers (giving them as much control as feasible), facilitate compliance in the private sector, preempt the patchwork of conflicting state laws, centralize enforcement at the Federal Trade Commission (FTC) and state Attorneys General (AGs), and continue to allow for the informed decision-making provided by market research, insights and analytics services.

A federal privacy bill needs to shift the burden away from consumers with a common set of transparency and privacy norms backed by strong enforcement to incentivize and ensure accountability by the businesses and organizations that utilize data every day. This model would:

- cover both for-profit companies and nonprofit organizations that, during a calendar year, control or process personal information of a substantial number of individuals, or that derive a significant portion of their gross revenue from the sale or other commercialization of personal information;
- avoid overly-restrictive prohibitions, while requiring contracts (with built-in oversight) between data-sharing partners to ensure clear responsibilities and consumer protection;
- include the privacy requirements common to state laws – notice and the rights to access, deletion, correction, portability, and opt-out -- with reasonable verification procedures;
- require reasonable & suitable data security practices, prioritizing general outcomes instead of specific technologies or approaches;
- prohibit specifically-defined unreasonable data practices, such as: using personal data to determine ineligibility for employment, credit, insurance, health care, financial aid, or housing (discrimination); charging a consumer a higher price for products/services based on personal data relating to the consumer's race, ethnicity, religion, national origin, sexual orientation or gender identity (except as permitted by existing laws applicable to the business/organization); impersonation for collection of personal data or obtaining access to a consumer's accounts, for purposes of fraud; misrepresenting/mischaracterizing products/services to induce disclosure of personal data; using personal information to defraud a consumer; using personal data in pursuit of criminal activity; or retaliating against a consumer for exercising their privacy rights;
- define personal data as "any information that is linked or reasonably linkable to an identified or identifiable individual," excluding aggregated, de-identified, and publicly available data;
- demand consent for action regarding personal data that is truly "sensitive";
- make exceptions for pseudonymous data,[1] and for routine and essential data practices;
- ensure allowable uses for "targeted advertising" don't restrict audience measurement;
- require assessments of data practices & risks, to see if the privacy costs would be outweighed by the countervailing benefits to the consumer or to competition, including determining significant risk of harm to consumers, benefits provided, the impact on a business's practices, consumers' reasonable expectations, and whether risk is being mitigated; and
- facilitate FTC-approved self-regulatory compliance programs and standards, such as ISO, to help police the marketplace, and encourage responsible data use (with participants in good standing getting the benefits of some protections from enforcement action).

[1] "**Pseudonymous data**" is typically defined as "personal information that cannot be attributed to a specific natural individual without the use of additional personal information, provided that such additional personal information is kept separately and is subject to appropriate technical and organizational measures to ensure that the pseudonymous data is not attributed to an identified individual."