IA Privacy Principles For A Modern National Regulatory Framework

Data has revolutionized every part of our economy and our lives, both online and offline. Businesses and nonprofits of all sizes, in all sectors, have integrated data into their products and services to the benefit of consumers.

Internet companies support an American approach to federal privacy legislation. Internet Association proposes six key principles to modernize national privacy legislation and regulation. These principles serve as the basis for ongoing conversations with stakeholders.

1. **Transparency.** Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared.

2. **Controls.** Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, unless that information is legally required, or is necessary for the basic operation of the business.

3. **Access.** Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to users.

4. **Correction.** Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.

5. **Deletion.** Individuals should have the ability to request the deletion of the personal information they provide to companies when it's no longer necessary to provide services, except where companies have a legitimate need or legal obligation to maintain it.

6. **Portability.** Individuals should have the ability to take the personal information they have provided to one company and provide it to another company that provides a similar service.

HOW DATA HELPS CONSUMERS AND MAIN STREET

Better curated recommendations for movies, TV shows, music, and restaurants

High-value targeted advertising and fundraising for small business owners and nonprofits

More personalized and convenient shopping experiences online and offline

Key Components Of A National Privacy Framework

Fostering privacy and security innovation. A national framework should not prevent companies from designing and implementing internal systems and procedures that enhance the privacy of each individual's personal information. Companies should take into account privacy and data security when they design and update their services, for example, by de-identifying, pseudonymizing, or aggregating data.

A national data breach notification law. A national framework should specifically preempt the patchwork of different data breach notification laws in all 50 states and the District of Columbia to provide consistency for individuals and companies alike. This national standard should protect individuals and their personal information through clear notifications, define a harm-based trigger for notification to avoid notice fatigue, and allow companies flexibility in how they notify individuals of unauthorized access to their personal information.

Technology and sector neutrality. A national privacy framework should include protections that are consistent for individuals across products and services. Such a framework should be both technology neutral (no specific technology mandates) and sector neutral (applying to online and offline companies alike).

Performance standard-based approach. A national privacy framework should focus on accomplishing privacy and data security protections, but laws and regulations should avoid a prescriptive approach to doing so, as such an approach may not be appropriate for all companies and may well become obsolete in light of rapidly developing technology.

Risk-based framework. A national privacy framework should be grounded in a risk-based approach, based on the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Consistent with FTC data security order provisions and the FTC's unfairness standard, companies should identify and address reasonably foreseeable risks to the privacy and the security of personal information where the result of failing to address the risk would cause, or be likely to cause, tangible consumer harm.

A modern and consistent national framework for individuals and companies. A national privacy framework should be consistent throughout all states, preempting state consumer privacy and data security laws. A strong national baseline creates clear rules for companies and ensures that individuals across the United States can expect consistent data protections from companies that hold their personal information. A national privacy framework should primarily be enforced by the FTC at the federal level and by state attorneys general at the state level, where the FTC declines to act.

ABOUT INTERNET ASSOCIATION

Internet Association represents over 40 of the world's leading internet companies. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. For more information, visit www.internetassociation.org