



THE ONLINE PRIVACY ACT

Americans still lack a comprehensive federal privacy law, leaving people with limited control over how their personal data is collected, used, and shared. As other countries and many states have acted, the U.S. remains without a national baseline. The Online Privacy Act would establish that baseline by creating enforceable user rights, clear limits and safeguards on data practices, and strong accountability for covered entities.

Key Provisions:

- **Digital Privacy Agency (DPA).** The bill creates a new federal agency to enforce users' privacy rights and ensure companies follow the law.
- **User Rights.** The bill gives users the right to:
 - access, correct, delete, and transfer data about them;
 - request a human review of impactful automated decisions;
 - opt-in consent for using data for machine learning / A.I. algorithms;
 - be informed if a covered entity has collected your information; and
 - choose for how long their data can be kept.
- **Company Obligations.** Companies must:
 - articulate the need for and minimize the user data they collect, process, disclose, and maintain;
 - minimize employee and contractor access to user data;
 - not disclose or sell personal information without explicit consent;
 - not use third-party data to reidentify individuals;
 - not use private communications, (e.g., emails and web traffic) for ads or other invasive purposes;
 - not process data in a way that violates civil rights, e.g., employment discrimination;
 - only process genetic information in limited circumstances;
 - use objectively understandable privacy policies and consent processes, and may not use 'dark patterns' to obtain consent;
 - employ reasonable cybersecurity policies to protect user data; and
 - notify the agency and users of breaches and data sharing abuses.
- **Enforcement**
 - The DPA would be authorized to issue regulations to implement the bill and to impose fines for violations.
 - State attorneys general would also be empowered to bring civil actions to enforce the bill's requirements.
 - Individuals may sue for declaratory or injunctive relief; individuals (not acting collectively) may sue for damages.
 - Harmed individuals and States may appoint nonprofits to bring collective, private civil actions for damages on behalf of users.
- **Protections for Journalists.** Expressly allows journalists to use or disclose personal information for investigative journalism no differently than they do today. This applies so long as there are safeguards against using the information for non-journalistic purposes.
- **Additional Provisions.** The bill criminalizes doxxing; limits companies from using data to build behavioral profiles without consent; exempts small businesses from the most onerous requirements.