Center for Digital Democracy's Principles for U.S. Privacy Legislation

Protect Privacy Rights,
Advance Fair and Equitable Outcomes,
Limit Corporate Practices and
Ensure Government Leadership and Enforcement

The Center for Digital Democracy provides the following recommendations for comprehensive baseline Federal privacy legislation. We are building on our expertise addressing digital marketplace developments for more than two decades, including work leading to the enactment of the 1998 Children's Online Privacy Protection Act--the only federal online privacy law in the United States. Our recommendations are also informed by our long-standing trans-Atlantic work with consumer and privacy advocates in Europe, as well as the General Data Protection Regulation.

We are alarmed by the increasingly intrusive and pervasive nature of commercial surveillance, which has the effect of controlling consumers' and citizens' behaviors, thoughts, and attitudes, and which sorts and tracks us as "winners" and "losers." Today's commercial practices have grown over the past decades unencumbered by regulatory constraints, and increasingly threaten the American ideals of self-determination, fairness, justice and equal opportunity. It is now time to address these developments: to grant basic rights to individuals and groups regarding data about them and how those data are used; to put limits on certain commercial data practices; and to strengthen our government to step in and protect our individual and common interests vis-à-vis powerful commercial entities.

We call on legislators to consider the following principles:

1) **Privacy protections should be broad: Set the scope of baseline legislation broadly and do not preempt stronger legislation**
   Pervasive commercial surveillance practices know no limits, so legislation aiming to curtail negative practices should
   a) address the full digital data life-cycle (collection, use, sharing, storage, on- and off-line) and cover all private entities' public and private data processing, including nonprofits;
   b) include all data derived from individuals, including personal information, inferred information, as well as aggregate and de-identified data;
   c) apply all Fair Information Practice Principles (FIPPs) as a comprehensive baseline, including the principles of collection and use limitation, purpose specification, access and correction rights, accountability, data quality, and confidentiality/security; and require fairness in all data practices.
   d) allow existing stronger federal legislation to prevail and let states continue to advance innovative legislation.

2) **Individual privacy should be safeguarded: Give individuals rights to control the information about them**
    a) Building on FIPPs, individuals ought to have basic rights, including the right to
        - transparency and explanation
        - access
        - rectification
        - erasure
        - object and restrict
        - portability
        - use privacy-enhancing technologies, including encryption
        - redress and compensation

3) **Equitable, fair and just uses of data should be advanced: Place limits on certain data uses and safeguard equitable, fair and just outcomes**

Relying on "privacy self-management"—with the burden of responsibility placed solely on individuals alone to advance and protect their autonomy and self-determination—is not sufficient. Without one's knowledge or participation, classifying and predictive data analytics may still draw inferences about individuals, resulting in injurious privacy violations—even if those harms are not immediately apparent. Importantly, these covert practices may result in pernicious forms of profiling and discrimination, harmful not just to the individual, but to groups and communities, particularly those with already diminished life chances, and society at large. Certain data practices may also unfairly influence the behavior of online users, such as children.

Legislation should therefore address the impact of data practices and the distribution of harm by

a) placing limits on collecting, using and sharing sensitive personal information (such as data about ethnic or racial origin, political opinions/union membership, data concerning health, sex life or sexual orientation, genetic data, or biometric data) or data that reveals sensitive personal information, especially when using these data for profiling;
b) otherwise limiting the use of consumer scoring and other data practices, including in advertising, that have the effect of disproportionally and negatively affecting people's life chances, related to, for example, housing, employment, finance, education, health and healthcare;
c) placing limits on manipulative marketing practices;
d) requiring particular safeguards when processing data relating to children and teens, especially with regard to marketing and profiling.

4) **Privacy legislation should bring about real changes in corporate practices: Set limits and legal obligations for those managing data and require accountability**
Currently companies face very few limitations regarding their data practices. The presumption of "anything goes" has to end. Legislation should ensure that entities collecting, using, sharing data
    a) can only do so for specific and appropriate purposes defined in advance, and subject to rules established by law and informed by data subjects' freely given, specific, informed and unambiguous consent; for the execution of a contract, or as required by law; and without "pay-for-privacy provisions" or "take-it-or leave it" terms of service.
    b) notify users in a timely fashion of data transfers and data breaches, and make consumers whole after a privacy violation or data breach;
    c) cannot limit consumers' right to redress with arbitration clauses;
    d) are transparent and accountable, and adopt technical and organizational measures, including
        i. provide for transparency, especially algorithmic transparency,
        ii. conduct impact assessments for high-risk processing considering the impact on individuals, groups, communities and society at large,
        iii. implement *Privacy by Design and by Default,*
        iv. assign resources and staff, including a Data Protection Officer,
        v. implement appropriate oversight over third-party service providers/data processors,
        vi. conduct regular audits
    e) are only allowed to transfer data to other countries/international organizations with essentially equivalent data protections in place.

5) **Privacy protection should be consequential and aim to level the playing field: Give government at all levels significant and meaningful enforcement authority to protect privacy interests and give individuals legal remedies**
Without independent and flexible rulemaking data-protection authority, the Federal Trade Commission has been an ineffective agency for data protection. An agency with expertise and resources is needed to enforce company obligations. Ongoing research is required to anticipate and prepare for additionally warranted interventions to ensure a fair marketplace and a public sphere that strengthens our democratic institutions. Legislation should provide
    a) for a strong, dedicated privacy agency with adequate resources, rulemaking authority and the ability to sanction non-compliance with meaningful penalties;
    b) for independent authority for State Attorneys General;
    c) for statutory damages and a private right of action;
    d) for the federal agency to establish an office of technology impact assessment that would consider privacy, ethical, social, political, and economic impacts of high-risk data processing and other technologies; it would oversee and advise companies on their impact-assessment obligations.