THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES

The United States confronts a crisis. Digital giants invade our private lives, spy on our families, and gather our most intimate facts for profit. Bad actors, foreign and domestic, target the personal data gathered by U.S. firms, including our bank details, email messages, and Social Security Numbers.

Our privacy laws are decades out of date. We urgently need a new approach to privacy protection. We must update federal laws and create a data protection agency specifically tasked with safeguarding the privacy of Americans. The time is now.

1. ENACT BASELINE FEDERAL LEGISLATION

We call for federal baseline legislation that ensures a basic level of protection for all individuals in the United States. We oppose the preemption of stronger state laws. U.S. privacy laws typically establish a floor and not a ceiling so that states can afford protections they deem appropriate for their citizens and be "laboratories of democracy," innovating protections to keep up with rapidly changing technology.

2. ENFORCE FAIR INFORMATION PRACTICES (FIPS)

Baseline federal legislation should be built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines. These frameworks create obligations for companies that collect personal data and rights for individuals. Core principles include:

- Transparency about business practices
- Data collection and use limitations
- Data minimization and deletion
- Purpose specification
- Access and correction rights
- Accountability
- Data accuracy
- Confidentiality/security

"Personal data" should be broadly defined to include information that identifies, or could identify, a particular person, including aggregate and de-identified data.

Federal law should also:

- Establish limits on the collection, use and disclosure of personal data,
- Establish enhanced limits on the collection, use and disclosure of data of children and teens,
- Regulate consumer scoring and other business practices that diminish people's life chances, and
- Prohibit or prevent manipulative marketing practices.

3. ESTABLISH A DATA PROTECTION AGENCY

Many democratic nations have a dedicated data protection agency with independent authority and enforcement capabilities. While the Federal Trade Commission (FTC) helps to safeguard consumers and promote competition, it is not a data protection agency. The FTC lacks rulemaking authority. The agency has failed to enforce the orders it has established. The US needs a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. The agency should also examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations. Federal law must establish a data protection agency with resources, rulemaking authority and effective enforcement powers.

4. ENSURE ROBUST ENFORCEMENT

Robust enforcement is critical for effective privacy protection. Arbitration clauses do not protect consumers and permit dangerous business practices to continue. If a company violates federal privacy law, consumers must be able to pursue a private right of action that provides meaningful redress without a showing of additional harm. Statutory damages are an essential element of an effective privacy law. Robust enforcement also requires independent action by State Attorneys General.

5. ESTABLISH ALGORITHMIC GOVERNANCE TO ADVANCE FAIR AND JUST DATA PRACTICES

The use of secret algorithms based on individual data permeates our lives. Concerns about the fairness of automated decision-making are mounting as artificial intelligence is used to determine eligibility for jobs, housing, credit, insurance, and other life necessities. Bias and discrimination are often embedded in these systems yet there is no accountability for their impact. All individuals should have the right to know the basis of an automated decision that concerns them. And there must be independent accountability for automated decisions. Protecting algorithms as a trade secret overprotects intellectual property and creates a barrier to due process. Trade agreements should uphold algorithmic transparency. Algorithmic transparency is central to algorithmic accountability.

6. PROHIBIT "TAKE IT OR LEAVE IT" TERMS

Individuals cannot have meaningful control of their personal data if the terms of service require them to waive their privacy rights. Furthermore, requiring individuals to pay more or receive lower quality goods or services if they do not waive their privacy rights is unfair and discriminates against those with less means. Federal law should require that consent, where appropriate, is meaningful, informed, and revocable, and should prohibit "pay-for-privacy provisions" or "take-it-or leave it" terms of service.

7. PROMOTE PRIVACY INNOVATION

Federal law should require innovative approaches to privacy and security, including strong encryption, robust techniques for deidentification and anonymization, and privacy enhancing techniques that minimize or eliminate the collection and disclosure of personal data, and make privacy by design an affirmative obligation. The consolidation of personal data with a small group of firms has stifled innovation and competition. Antitrust enforcement agencies should consider privacy interests in merger review. Mergers that fail to protect the privacy of consumers should be rejected.

8. LIMIT GOVERNMENT ACCESS TO PERSONAL DATA

Personal data held by companies are often sought by government agencies for law enforcement purposes. We do not object to the disclosure of specific records that are required for legitimate criminal investigations and obtained through an appropriate judicial procedure. However, there should be a clear standard in a privacy law for such disclosure. U.S. companies cannot disclose user data in bulk to government agencies.

Signed,
Americans for Financial Reform
Berkeley Media Studies Group
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Center for Media Justice
Color of Change
Consumer Action
Consumer Federation of America
Defending Rights & Dissent
Electronic Privacy Information Center
Media Alliance
Parent Coalition for Student Privacy
Privacy Rights Clearinghouse
Privacy Times
Public Citizen
Stop Online Violence Against Women
U.S. PIRG