THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL JUSTICE 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. Through a vast, opaque system of algorithms, we are profiled and sorted into winners and losers based on data about our health, finances, location, gender, race, and other personal information. The impacts of this commercial surveillance system are especially harmful for marginalized and multi-marginalized communities, fostering discrimination and inequities in employment, government services, health and healthcare, education, and other life necessities.

The lack of a U.S. privacy law places not only our individual autonomy, but our democracy at risk. We need a comprehensive baseline federal privacy and digital justice law with strong enforcement. The time is now.

LIMIT THE COLLECTION AND USE OF PERSONAL DATA

Federal legislation should move away from "notice and choice" frameworks and instead place strict limits on the collection, use, storage, and transfer of personal data. Data collection and use should be limited to what is reasonably necessary to provide a good or service requested by an individual in an intentional interaction. Purpose specification should be strictly enforced. "Personal data" should be broadly defined to include information that is linked to or could be linked to a particular person, household, or device.

Federal legislation should build on the U.S. Code of Fair Information Practices and OECD Privacy Guidelines, which are widely followed and form the basis of other data protection regimes. These frameworks create obligations for companies that collect personal data and give rights to individuals. Core principles include:

- Strict data collection and use limitations
- Data minimization and deletion requirements
- Transparency about business practices
- Purpose specification
- Access, correction, and deletion rights
- Data accuracy
- Confidentiality and security requirements
- Compliance and accountability

Some types of data, and some uses of data, are especially sensitive and deserve strict regulation. For instance, biometric and genetic data are inherently sensitive, but even information about the products people buy and the services they search for can be used to make inferences about their health, religious beliefs, economic situations, and other characteristics that are sensitive in nature. In these situations, requiring express, affirmative opt-in consent or prohibiting certain data collection and use may be necessary. Data should be deleted after it is used for the disclosed purpose. Federal law should also establish enhanced digital safeguards for children and teens, including safeguards against age-inappropriate marketing practices.

PROHIBIT DISCRIMINATORY USES OF DATA

Privacy legislation should protect against discriminatory uses of data. It should extend civil rights protections online and require robust algorithmic assessments. It should prohibit predatory data collection practices and uses. Processing that leads to disparate treatment or adverse disparate impacts should be prohibited. Technology that increases the surveillance of communities of color, like facial recognition, should be banned.

PROVIDE FOR A PRIVATE RIGHT OF ACTION

Robust enforcement is critical for effective privacy protection. The inclusion of a private right of action with statutory damages is a crucial tool to supplement government enforcement, particularly for marginalized communities. If a company violates federal privacy law, individuals and groups of individuals, or their agents, should be able to pursue a private right of action that provides meaningful redress without a showing of additional harm. Congress should also grant enforcement authority to State Attorneys General.

PRESERVE STATES' RIGHTS TO ENACT STRONGER PROTECTIONS

We call for federal baseline legislation that ensures a basic level of protection and advances digital justice for all individuals in the United States. We oppose the preemption of stronger state laws. U.S. privacy laws typically establish a floor so that states can provide protections they deem necessary for their citizens and be "laboratories of democracy," innovating protections to keep up with rapidly changing technology.

ESTABLISH A DATA PROTECTION AGENCY

The U.S. needs an independent Data Protection Agency dedicated to privacy and data protection, oversight, and enforcement, with the authority and resources to address emerging privacy challenges. Congress should allocate additional resources to regulate this massive sector of the U.S. economy. The DPA should have the expertise necessary to address the threats technology can pose to civil rights, individual autonomy, and democracy. The DPA should examine the social, ethical, and economic impacts of data processing and oversee compliance and impact-assessment obligations. The DPA should work with antitrust agencies to address competition and growing concentration in the technology sector by reviewing and issuing guidance on the privacy and data protection implications of proposed mergers. Congress should empower a DPA with adequate resources, rulemaking authority, and effective investigatory and enforcement powers.

REQUIRE ALGORITHMIC FAIRNESS AND ACCOUNTABILITY

The use of algorithms and artificial intelligence systems pose significant risks to fundamental rights. Public and private actors are increasingly using AI systems to make decisions about eligibility for jobs, education, housing, parole and bail, credit, insurance, healthcare, and government services. The error, bias, and discrimination embedded in these systems perpetuate systemic inequities, yet there is no accountability for their impact. Personal data collection and processing is not the only issue in this context – aggregate and de-identified data is often used to make determinations that adversely affect individuals and groups. Federal law should require continuous, independent oversight over algorithmic decision-making with transparent algorithmic impact assessments, random audits, and other public accountability mechanisms. It should require a right to human review of automated decisions. Uses of AI that subvert human and civil rights should be prohibited, such as uses in the criminal justice system or for mass surveillance.

BAN MANIPULATIVE DESIGN AND UNFAIR MARKETING PRACTICES

Privacy legislation should prohibit "dark patterns" designed to manipulate individuals into making choices that are in the businesses' interests rather than their own. Pay-for-privacy provisions or take-it-or-leave-it terms of service, which discriminate against those with less means, should be illegal.

LIMIT GOVERNMENT ACCESS TO PERSONAL DATA

Any government collection of personal data should have a lawful basis, be performed in accordance with applicable data protection laws, be limited in time and scope to the original purpose of collection, and be subject to independent oversight. With few exceptions, it should be conducted only with the consent of those whose personal data is collected. Personal data should not be collected in bulk, from third-party data brokers without a warrant, or through warrantless surveillance. Agencies should appoint a Chief Privacy Officer at the leadership level with the authority to oversee and address privacy issues across the agency.

Center for Digital Democracy
Color of Change
Consumer Action
Consumer Federation of America
Electronic Privacy Information Center
Fairplay
Parent Coalition for Student Privacy
Parents Together Action
Privacy Rights Clearinghouse
Public Citizen
U.S. PIRG