Computer & Communications
Industry Association
Tech Advocacy Since 1972

PRIVACY PRINCIPLES:

A New Framework for Protecting Data and Promoting Innovation

Purpose

As the world becomes increasingly data-focused, attention has inevitably shifted to the impact of data on consumers and whether and how improvements should be made. Recent controversies have shifted how companies and consumers think about how data is collected and used online, generating some positive responses in terms of practice and transparency. It is important for the U.S. to have a healthy data ecosystem with transparency and accountability, which will help drive innovation and U.S. competitiveness.

CCIA supports the development of baseline, Federal privacy legislation that would ensure that data is handled responsibly and with transparency while also ensuring that individuals can benefit from innovation and new technologies. Such a framework should be technology-neutral, meaning it should not provide specific technology mandates; sector-neutral, meaning it should apply to online and offline organizations; and it should provide for safe harbors and flexibility for organizations to make adjustments according to the needs of individuals and evolving technology. CCIA presents these "Privacy Principles" to help guide the development of a national policy on consumer privacy.

Policy Overview

These principles aim to protect data through a robust, technology-neutral framework for assessing and managing privacy risks to individuals and organizations, and to promote innovation, in both digital services and privacy protection. Organizations across the digital ecosystem use personal data to provide innovative services. Responsible data use can be beneficial for people, businesses, and society. Reasonable data protection measures that align with individuals' expectations can protect people and communities from harms that result from misuse of data and help maintain the trust that enables the digital economy.

When evaluating the reasonability of an organization's data protection practices, it is important to understand the context in which an organization collects, processes, and uses personal information. This context can include the nature of the relationship between an individual and the organization; the potential benefits an individual, organization, and society might receive from particular uses of information; and individuals' expectations regarding data protection.

Individuals depend on organizations to use their data responsibly and be transparent about what they are collecting and how they are collecting and using it. Therefore, organizations must respect individuals' interests when they process personal information. Organizations should make reasonable best efforts to account for and mitigate potential harms to individuals, communities, and society.

Scope and Definitions

Personal information or data include any data under the control of a covered organization, that is not de-identified or otherwise generally available to the public through lawful means, and is linked or practically linkable to a specific individual, or linked to a specific device or account that is associated with or routinely used by an individual.

Different types of personal data can vary in sensitivity, depending on the context. However, some personal data is almost always sensitive. This includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, and certain data of known minors.

Privacy risk
The potential for personal information, on its own or when linked to other information that might identify an individual, to cause economic loss, discrimination, exclusion, loss of self determination, or physical, reputational, or professional harm to an individual.

Covered organizations or entities include all organizations that process personal information regardless of whether they have a direct or commercial relationship with an individual whose information they hold.

Proportionality
Reasonable data protection practices may differ across covered organizations. Context, including an organization's scale and resources, the sensitivity of the data it holds, and its uses for that data, should inform the measures that it puts in place to protect data.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

Interoperability
Cross-border data flows are essential to the modern economy. Organizations and individuals benefit from consistent compliance programs based on widely shared principles of data protection. These principles are intended to be interoperable and consistent with existing cross-border data transfer mechanisms, industry standards, and other cross-organization cooperation mechanisms.

Requirements for Organizations

Control
Covered organizations must provide appropriate mechanisms for individual control, considering the service. Individuals should be able to object to data processing where it is feasible, but specific consent should not be mandatory for every aspect of data processing, which could create an overly complex and confusing experience for the individual and divert from the overall goals that the policy seeks to achieve. Policymakers should also keep in mind that the responsible processing of personal information is necessary to simply operate some services.

Access
Individuals must be able to access the personal information that they have provided to a covered organization, and it should be made available for export in a machine-readable format.

Accuracy
Personal information should be accurate, current, and complete to the extent possible for the purpose for which the covered organization maintains the data.

Deletion
Pursuant to the above "Access" principle, covered organizations should afford users with the ability to correct and/or delete the data that they provide to that organization when it would be practical and provided that deletion would not implicate the personal information of others.

Portability
Covered organizations should make reasonable efforts to enable authenticated users to obtain data they provide to that organization for their own purposes or for use with a different organization or service, provided that these data portability tools do not implicate the personal information of others. Data transfers between covered organizations should be private, secure, and balanced. Data portability tools should: (1) allow users to download and move data they have provided to the service, but not data that may relate to other users; (2) afford users control over how and when the tools are used; and (3) be tailored to the privacy and security expectations of specific products and services. Further, data portability tools should enable machine-to-machine transfers where technically feasible.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534

Security and Integrity
Users should expect that organizations handling their data will do so carefully and responsibly with reasonable measures to protect personal information from unauthorized access, misuse, modification, disclosure, loss, and destruction. Policy should account for and be proportionate to the risk of harm. Organizations should follow consensus best practices, and if a security breach occurs, organizations should notify individuals expeditiously when there is a significant risk of harm.

Onward Transfers
Covered organizations should ensure that personal information that they collect or process is protected in a manner consistent with the above principles even if it is transferred to third parties. Covered organizations should use enforceable mechanisms and independent audits to ensure that third parties protect data according to these principles.

Accountability

Transparency
Covered organizations must be transparent about the types of personal information that they are collecting and how they are collecting and using it. Covered organizations should be clear about whether the personal information may be transferred to third parties, how long information may be retained, and what choices and controls individuals have with respect to their personal information. Covered organizations should make reasonable efforts to actively inform individuals, making the information relevant and actionable, about data use in the context of the relevant services.

Accountability
Covered organizations should be held accountable for meeting the requirements set out in these Privacy Principles. Covered organizations should regularly assess the privacy risks associated with their collection, processing, and use of personal information; develop systems to mitigate risks in a reasonable and proportionate manner; and monitor services for bias and disparate impacts. Organizations should practice privacy by design, building products and services that prioritize privacy, security, reliability, and reduce the likelihood of vulnerabilities, which will help earn user trust. Policymakers should set baseline requirements but enable flexibility to meet those requirements and promote industry accountability programs and safe harbors.

Enforcement
A robust federal baseline would provide clear standards for covered organizations and ensure that individuals across the United States can expect consistent data protections from organizations that retain their data. A national, privacy framework should be consistent throughout the United States, so state laws concerning data privacy, security, and breach notifications should be preempted where appropriate. This framework should be enforced primarily by the FTC at the federal level, but it should allow for enforcement by state attorneys general where the FTC has declined to act.

CCIA | 655 15th St NW #410 | Washington, DC 20005 | ccianet.org | Phone: +1 (202) 783-0070 | Fax: +1 (202) 783-0534