Centre for Information Policy Leadership
HUNTON

Ten Principles for a U.S. Privacy Law

April 2024

Ten Principles for a U.S. Privacy Law

Data has long been a critical asset across the economy, but the use of personal information, in particular, has garnered greater attention in the age of data-driven technologies such as Artificial Intelligence (AI). AI has brought into sharp focus the question of how we should regulate and govern the use of personal data to advance the economy and reap the benefits of innovation while building trust and mitigating potential harms to individuals from the use of their data. In response to these challenges, many legislatures at the state level have updated or are creating their data privacy laws and frameworks. This has created a patchwork of protections for individuals and divergent compliance obligations for U.S. businesses that could hinder the ability to leverage data effectively across the U.S. for data-driven innovation and economic progress.

The Centre for Information Policy Leadership (CIPL) believes that a federal baseline privacy law can be more effective in establishing consistent privacy protections for individuals and legal obligations for organizations than is possible through the current state law patchwork. In addition, and importantly, a federal privacy law should have the objective of enabling data use for innovation in the digital economy to further advance U.S. leadership and competitiveness.

CIPL believes that the following principles will help ensure that these goals are met:

1. Organizational Accountability

Organizational Accountability is a key building block of modern data protection in the age of digital transformation and should be a core feature of a federal privacy law. It requires organizations to:

- take necessary steps to implement applicable data protection requirements or other privacy standards through outcomes-based and risk-based privacy programs; and
- be able to demonstrate such implementation on request.

A federal U.S. law should require organizations to implement accountability-based privacy programs, either independently or through formal accountability schemes such as codes of conduct and certifications (e.g., Global Cross-Border Privacy Rules and Global Privacy Recognition for Processors) that cover all the necessary elements of accountability. CIPL's Accountability Framework features these elements, i.e., leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, and response and internal enforcement and has been used by both regulators and companies as a blueprint for effective and accountable AI and data governance programs (see Figure 1 below).

Accountability is a more flexible instrument than prescriptive requirements and therefore better suited in the era of fast-paced technological developments. It enables organizations to apply legal rules and implement data protection principles flexibly and proportionately to their size, context of data use, and risks. They would avoid the application of overly prescriptive measures where risks are low. Organizations can focus on outcomes of what must be achieved, without having to comply with burdensome legal requirements prescribing how to achieve them. Importantly, an accountability-based approach would hold organizations responsible for ensuring that appropriate privacy protections will continue to apply to personal data across the digital ecosystem, wherever data goes.

A federal data privacy law should also *incentivize* organizational accountability and privacy programs. This would ensure their robustness and encourage companies to invest in accountability and digital trust, which is necessary for the adoption of new technologies, products, and services. The use of demonstrated accountability measures should be recognized as a mitigating factor in enforcement or as an advantage in a procurement process, for example.

Figure 1

2. Risk-Based Approach

Harm prevention while enabling the benefits of data use should be a key focus of a federal privacy law. A risk-based approach to privacy facilitates this focus on harm and benefit, as it requires organizations to assess the risks of harm to individuals and the benefits that are associated with the specific uses of personal information. It also enables risk mitigations that are tailored to the specific risk/benefit assessment. This approach places the primary burden of protecting consumers directly where it belongs—on the organizations using personal information.

Accordingly, a U.S. privacy law should take a flexible, risk-based approach that enables calibration of legal requirements and compliance measures to the actual risks to individuals that are associated with or could flow from the intended uses of personal information. This approach would at the same time take into account the benefits of data use and the risks of not using data in a specific context, i.e., the risk of loss of opportunity. It will also help smaller organizations and start-ups avoid taking on unnecessary administrative burdens by allowing them to scale and calibrate their compliance based on actual risks and benefits. Importantly, a risk-based approach also ensures that the law is technology-neutral and future proof, as an appropriate risk/benefit assessment process can be applied to any current and future technology, data uses, and business practices.

This approach should describe the types of risks that should be considered and what might constitute high risk. Similarly, obligations should be flexible enough to enable low risk use cases such as fraud prevention . In most cases, any guidance should also enable organizations to rebut a presumptive classification of a given data processing activity as high risk. Such an approach provides organizations with the ability to innovate actual controls, technical tools, and safeguards, while maintaining consistency with core privacy principles and outcomes.

3. Contextual Transparency

Informing individuals about what happens with their data is essential for building trust in the digital economy. That said, in modern digital contexts, individuals are often provided with overly complex, legalistic, and long privacy notices that are effectively meaningless.

A federal privacy law offers the opportunity for setting a new standard for transparency that is user-centric, contextual, and tailored towards specific data uses and audiences, including both push and pull models, proactive notices, and on-demand information. There should be an obligation to provide basic information to individuals where data uses, recipients, and broader purposes of processing may not be obvious to individuals, along with essential information about any choices that may be available, complaint and redress options, whom to contact for more information, etc. Organizations must be allowed the flexibility to provide additional transparency, as needed, in a layered and user-centric format.

4. Individual Protections

Empowering individuals to participate in the decisions about how their personal information is used, including through access and correction rights, has formed part of the U.S. approach to privacy. While choice and consent were intended to give individuals control over their information, empowering individuals in today's digital landscape is vastly different from the time when these concepts were introduced. A federal privacy law should include a robust set of individual rights. While choice and consent should remain available in contexts where they are effective and appropriate, individual participation through consent will not always be effective or appropriate in today's complex digital economy. For example, obtaining consent may not be possible, effective or appropriate in the context of fraud prevention. Failing to distinguish between situations where choice and consent are effective and where they are not will lead to consent fatigue and ultimately undermine the very purpose of empowering individuals.

Real empowerment can be delivered through other accountability measures, such as demonstrable risk-based protections, anonymization or de-identification of personal information, complaint-handling and redress mechanisms, as well as the rights of access, correction, deletion, and opt-out of certain processing, where appropriate and feasible.

5. Controller and Processor Distinction

It is important to distinguish between the obligations of "controllers" that collect and determine the uses of personal information and "processors," typically vendors or service providers, that provide some service with respect to personal information on behalf of controllers. This distinction is important for at least two reasons:

- It will eliminate confusion around the respective statutory requirements applicable to controllers and processors. Controllers typically determine the intended uses of personal information and are responsible for ensuring compliance with all legal requirements pertaining to the processing of personal information. Controllers are also typically the ones that have a direct relationship with individuals. Processors typically process personal information to provide a specific service to and on behalf of controllers pursuant to a contract that defines their obligations. In certain contexts, such as for business operational purposes including product improvement, security, and fraud prevention, data processors should also have appropriate rights to use personal information for their own business purposes in a way that benefits and protects the privacy of consumers (in-line with reasonable expectations of the consumer). Otherwise, if processors use data for their own purposes, they become controllers in their own right. Processors act on behalf of controllers and follow the requirements specified by controllers. Controllers are responsible for complying with all substantive requirements set forth in a privacy law, including requirements relating to permissible uses of personal information, individual rights such as access and correction, as well as notice and choice requirements. The direct statutory requirements on processors are typically limited to ensuring reasonable data security and to implementing the relevant contractual requirements specified by the controllers.

- It is the prevailing global practice to distinguish between and specify controller and processor obligations in data privacy laws. Some U.S. sectoral laws, such as HIPAA, also recognize the distinction. Many multinational organizations are increasingly exposed to these concepts and have learned to work with them and address them both contractually and in privacy compliance program controls. Following a similar approach in the U.S. would enhance global interoperability. More importantly, it would help streamline and rationalize the compliance efforts by multinational and other organizations providing services globally and would help prevent overlapping and conflicting compliance efforts by controllers and processors. It would also avoid confusion and legal uncertainty that could lead to ineffective protections and diminished trust in the digital economy and, more specifically, in cloud and AI services.

That said, it is important that the controller/processor distinction be adaptable to the specific contexts of data use, including contexts where the distinction may not apply.

6. Global Interoperability

Global interoperability facilitates the responsible movement of data beyond borders, streamlines business operations, reduces the costs of implementation, and ensures efficient compliance across regions, thus supporting the continued growth of the digital ecosystem and the effective and beneficial use of personal data. The U.S. should design its federal privacy law in a way that takes into account as much as appropriate—and even helps to evolve—key concepts from major non-U.S. privacy laws to maximize interoperability between different legal and privacy regimes and decrease the compliance burdens on U.S. businesses.

With unprecedented volumes of data traveling and being accessed across borders, it is important for the U.S. to assert its digital leadership by creating efficient and reliable cross-border data transfer mechanisms that enable access to robust, globally sourced datasets for data-driven technologies, including AI. This includes ensuring that restrictions to cross-border flows of personal information are only instituted when necessary and are proportionate to the risks presented by the transfer, taking into account the type of data being transferred and the broader context of the cross-border transfer. Although cross-border data flows should be encouraged, they should

also be protected by holding the originating organization accountable for requiring the continued protection of data as it flows across borders. Organizations should be encouraged and incentivized to adopt mechanisms for trustworthy transfers like the Global Cross-Border Privacy Rules (Global CBPR).

7. Supportive of Innovation

Any federal privacy law should support and reward responsible innovation and societally beneficial uses of data that take into account privacy, effectively manage the associated risks, and ensure that data is used in an accountable way.

The U.S. is a world leader in innovation. Its federal law must ensure the U.S.'s continued ability to lead through flexible and technology-neutral measures and requirements that remain relevant and effective as technology, data uses, and business practices evolve, including through continued U.S. leadership in global standards bodies. It must not impose unnecessarily restrictive rules on any particular of technology, such as AI or machine learning, and it must facilitate the broad use and sharing of data for the benefit of both society and individuals.

A federal privacy law should promote and incentivize investment in and adoption of privacy-protective and privacy-preserving technologies. These techniques enable organizations to unlock the potential of data to drive innovation in developing products and services, while preserving digital trust and the value of data as a key business asset.

8. Oversight and Smart Regulation

Ideally, there should be a single, appropriately resourced, independent federal regulator responsible for regulatory oversight and enforcement under a U.S. federal privacy law. That regulator could be an existing federal agency, such as the Federal Trade Commission (FTC), which has deep expertise and experience with privacy oversight. In addition, State Attorneys General should also play a role in enforcing this law, subject to FTC leadership, guidance, and coordination to ensure consistency.

In enumerating regulatory powers and obligations, a federal privacy law should place emphasis on and prioritize regulatory leadership, engagement, and collaboration with organizations ahead of enforcement, for instance, through incentivizing organizational accountability and the development of innovative regulatory policy.

With respect to incentivizing accountability, both lawmakers and regulators must reward accountable organizations that are able to demonstrate their commitment to and implementation of comprehensive privacy management programs, including through formal certification schemes or by participation in codes of conduct. The regulatory incentives for implementing such programs can span a wide range of practices, including using demonstrated accountability as a mitigating factor or safe harbor in enforcement contexts, reducing certain regulatory burdens by providing license to engage in broader beneficial data uses, recognizing best practices, and using demonstrated accountability as evidence of due diligence in the contexts of selecting service providers and vendors for government procurement contracts, among many others.

Furthermore, regulatory oversight and enforcement agencies should be specifically encouraged to develop innovative regulatory approaches, policies, tools, and methodologies that are more appropriate to the agile and

fast-paced nature of the subject that they regulate. These can include regulatory sandboxes, iterative compliance reviews, innovation hubs for start-ups, and collaborative co-regulation efforts.

9. Effective and Proportionate Enforcement

While a U.S. federal privacy law should include sensible and meaningful penalties for violations, the law should enable and prioritize alternative approaches to traditional enforcement. Extreme and disproportionate penalty levels may have the unintended consequences of chilling innovation and encouraging selective punishment. Alternative approaches can include various forms of constructive *ex ante* engagement and collaboration between regulators and industry (see Oversight and Smart Regulation above) to identify potentially problematic products, services, and business practices, and the ability for regulators to issue orders mandating outcomes to be achieved, with fines being reserved for the most serious violations.

Even then, penalty processes and fines should be proportionate to the harm, taking into account a company's size, employees, revenue, profits, etc., and be reduced or mitigated for demonstrated accountability and compliance efforts. Penalties should only be a last resort to deal with negligent, willful, or systematic failures.

10. Comprehensive and Harmonized Law

The U.S. should craft a federal privacy law that affords U.S. businesses the advantage of a unified, large U.S. market, including in data and technology, that provides regulators and organizations with consistent rules and legal certainty, and that assures uniformly strong privacy protections to individuals, irrespective of state or industry. That law should provide comprehensive baseline privacy protections applicable to all industries and, where appropriate, amend or replace existing inconsistent state and federal privacy laws. The U.S. should develop a modern, risk-based, comprehensive horizontal law that regulates data use consistently across industries, with appropriate exceptions, as information is increasingly cross-sectoral, and data-driven innovation is premised on the ability to use data sets from different sectors.

This approach should preserve the qualified ability of individual states to enact their own privacy-related laws providing protection to individuals in areas not covered by the federal law, where appropriate and effective.