Centre for Information Policy Leadership
Hunton Andrews Kurth

21 March 2019

Ten Principles for a Revised US Privacy Framework

Our economies and societies are in the midst of the 4th industrial revolution, with digitalization and datafication transforming the way we live, work and interact. This transformation has brought into sharp focus the question of how we should regulate data use, governance and privacy to enable us to reap the benefits of data driven innovation while mitigating the risks associated with ubiquitous and massive data use. In response, many countries have updated or are in the process of updating their data privacy laws and frameworks. Some are introducing data protection and privacy requirements for the first time. The US has long regulated data in specific sectors. More recently, the US has started to follow the path toward generally applicable data protection regulation with the passage of the California Consumer Privacy Act (CCPA) in 2018, similar legislative proposals in other states and numerous proposals for a comprehensive federal privacy law by various groups, including federal legislators on both sides of the political spectrum.

The Centre for Information Policy Leadership (CIPL) believes that the use of personal information and privacy can be most effectively regulated at the federal level. Thus, the present paper focuses on principles for a potential US federal privacy law. This federal law should have the dual objectives of providing appropriate privacy protections for consumers and enabling the digital economy and innovation to ensure US leadership and competitiveness. CIPL believes that the following principles will help ensure that these dual goals are met.

1. Accountability

Accountability is a key building block of modern data protection. It requires organizations to:

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

A US law should require organizations to implement such accountability-based comprehensive privacy programs, either independently or through formal accountability schemes such as codes of conduct and certifications (e.g. APEC CBPR), that cover the full range of the necessary elements of accountability—leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and internal enforcement.

The law should also positively incentivize organizations to implement accountability-based privacy programs that go above and beyond minimum requirements. Such incentives should include using demonstrated accountability as a mitigating factor in enforcement.

Further, personal information transferred across borders should be encouraged to support global markets but also protected by holding the originating organization accountable for requiring the continued protection of data as it flows across the border.

2. Risk-based Approach

Harm prevention has been a key focus of privacy regulation in the US to date. A risk-based approach to privacy facilitates this focus on harm 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 burden of protecting consumers directly where it belongs—on organizations using personal information.

The revised US privacy framework should be based on a flexible risk-based approach that enables calibration of legal requirements and compliance measures to the actual risks to individuals associated with any given uses of personal information. This approach will also help smaller organizations and start-ups avoid unnecessary administrative burdens by allowing them to scale and calibrate their compliance based on risk to consumers. It 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 use and business practice.

The law should also enable the relevant federal privacy regulator(s), such as the Federal Trade Commission, to develop guidelines on what types of risks should be considered.

3. Innovative and Contextual Transparency

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

Revising the US privacy framework 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, who to contact for more information, etc. Organizations must be allowed the flexibility to provide any additional transparency based on the context of the envisioned data uses in a layered and user-centric format.

4. Individual Empowerment

Empowering individuals to participate in the decisions about how their personal information is used and through access and correction rights has formed part of the US approach to privacy from the start. Choice and consent have also played a prominent role in attempting 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 new US law should include a robust set of individual rights, and choice and consent should remain available in contexts where they are effective and appropriate. In today's complex data economy and our digital lives, individual participation through consent will no longer be effective or appropriate in many contexts. Failing to distinguish between situations where choice and consent are effective and where they are not will lead to consent fatigue and the illusion of empowerment.

Real empowerment for consumers can be delivered through other accountability measures, such as risk-based protections by the organizations, the requirement to demonstrate accountability measures, anonymization or de-identification of personal information, complaint handling and redress mechanisms, as well by individuals' rights of access, correction, objection and erasure, where appropriate.

5. Controller/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 permissible uses of personal information and are responsible for ensuring compliance with all legal requirements pertaining to the processing of data. Controllers are typically the ones that have the 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. If processors use data for their own purposes, they become controllers in their own right. Processors only 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 data, 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 US sectoral laws, such as HIPAA, also recognize the distinction. Many 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. This is especially true given the global nature of IT services and cloud computing technology and providers. Following a similar approach in the US would enhance global interoperability. More importantly, it would help streamline and rationalize the compliance efforts by multinational and other organizations (including many IT and technology service providers in the US) and 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.

However, it is important that the controller/processor distinction is adaptable to the specific contexts of data processing, including contexts where the distinction may not apply.

6. Global Interoperability

Rapid globalization and increase in digital trade have resulted in unprecedented volumes of data traveling or being accessed across borders and a plethora of national legislation designed to protect data that leaves its location of origin. In addition to harmonizing its domestic privacy legislation, the US should design its revised privacy framework in a way that harmonizes as much as appropriate with key concepts in major non-US privacy laws to maximize interoperability between different legal and privacy regimes. Global interoperability facilitates the responsible movement of data beyond borders, streamlines business, reduces the costs of implementation and delivers efficiencies in compliance across regions, thus supporting the continued growth of the digital ecosystem and the effective and beneficial use of personal data.

Interoperability does not require implementing the same law in every country. Each country must be able to approach legislation based on its own priorities and legal traditions. Thus, adopting a verbatim version of the European Union’s General Data Protection Regulation (GDPR) would not be appropriate. For example, US First Amendment principles and traditions may mean that the US should consider a unique approach to regulating data found in public government records or other publicly available data. Similarly, a new US privacy framework should not undercut data uses that may rely on personal information to actually protect consumers and the public interest, such as by furthering the fight against financial crimes, identity theft, modern slavery and other crimes. It also should not undercut the ability to innovate and to generally use data beneficially.

7. Supportive of Responsible Innovation

Any revised privacy framework should support and reward responsible innovation that takes into account privacy issues, effectively manages the associated risks and ensures that data is used in an accountable way. The US is a world leader in innovation. Its revised framework must ensure the US'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. It must not impose unnecessarily restrictive rules on any particular types of technology, such as artificial intelligence or machine learning, and it must facilitate the use of data for the benefit of both society and individuals.

8. Oversight and Smart Regulation

Ideally, there should be a single, appropriately resourced federal regulator responsible for regulatory oversight and enforcement under a federal US 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 play a role in enforcing this law, subject to FTC leadership, guidance and coordination to ensure consistency.

In enumerating regulatory powers and obligations under a new framework, the law should place emphasis on and prioritize regulatory leadership and 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 can range from using demonstrated accountability as a mitigating factor or safe harbor in enforcement contexts, to reducing certain regulatory burdens by providing license to engage in broader beneficial data uses, to public recognition of "best in class" practices, to using demonstrated accountability as evidence of due diligence in the contexts of selecting service providers and vendors or of government procurement contracts, among many other possible incentives.

Furthermore, regulatory oversight and enforcement agencies should be specifically encouraged to develop innovative regulatory policies 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 and collaborative co-regulation.

9. Effective Enforcement

While a new federal privacy framework 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. The alternatives can be various forms of constructive 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, take into account company size (employees, revenue, profits, etc.), be reduced or mitigated for demonstrated accountability and compliance efforts, and should only be a last resort to deal with negligence, willful or systematic failures.

10. Comprehensive and Harmonized Framework

The US should craft an approach that will capitalize on the large US digital market and that provides regulators and organizations with consistent rules and legal certainty, as well as uniformly strong privacy protections to consumers, irrespective of the state or industry. A harmonized framework must aim to preempt a patchwork of inconsistent state laws and thereby avoid a balkanized approached to US data regulation which could burden innovation directed at the US digital market, hamstring SMEs and new market entrants, as well as undermine consistent privacy protections for consumers. That framework should provide comprehensive baseline privacy protections applicable to all industries and, where appropriate, amend or replace existing inconsistent federal privacy laws, particularly where such existing laws fall below the new baseline. In expanding privacy protections, the US should thus depart from its traditional sectoral focus in privacy and develop a comprehensive horizontal framework 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.

If you have any questions or would like additional information about the above principles, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 74 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth LLP.