February 25, 2019

Chairwoman Jan Schakowsky and Ranking Member Cathy McMorris Rodgers
House Committee on Energy and Commerce
Rayburn House Office Building 2125
Washington, D.C. 20515

Dear Chairwoman Schakowsky and Ranking Member McMorris Rodgers:

Internet Association[1] (IA) welcomes the opportunity to submit this letter and our enclosed principles for a national privacy framework for the record as part of the Committee's February 26 hearing *"Protecting Consumer Privacy in the Era of Big Data."*

IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society and the economy and, as the voice of the world's leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits.

We appreciate the Committee holding this hearing to advance the conversation around an American approach to data privacy. Internet Association members support a modernized U.S. privacy framework that provides people meaningful control over their data across all industries, makes companies accountable, and includes meaningful enforcement. A globally respected American regulatory framework must prioritize protecting individuals' personal information and foster trust through meaningful transparency and control. We believe this can be done by empowering people to better understand and control how personal information they share is collected, used, and protected. People should also be able to access, correct, move, and delete their personal information except where there is a legitimate need or legal obligation to maintain it. Consumers deserve the right to control the use of their personal information, and we want to see the president sign a new law this year.

IA released privacy principles in support of an American approach to federal privacy legislation that is consistent nationwide, proportional, flexible, and enables companies to act as good stewards of personal information provided to them by individuals. IA's proposed principles include:

- **Transparency.** Individuals should have the ability to know if and how personal information they provide is used and shared, who it's being shared with, and why it's being shared.
- **Controls.** Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, unless that information is legally required, or is necessary for the basic operation of the business.
- **Access.** Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to individuals.
- **Correction.** Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- **Deletion.** Individuals should have the ability to request the deletion of the personal information they provide to companies when it's no longer necessary to provide services, except where companies have a legitimate need or legal obligation to maintain it.

[1] Internet Association represents https://internetassociation.org/our-members/.

- **Portability.** Individuals should have the ability to take the personal information they have provided to one company and provide it to another company that provides a similar service.

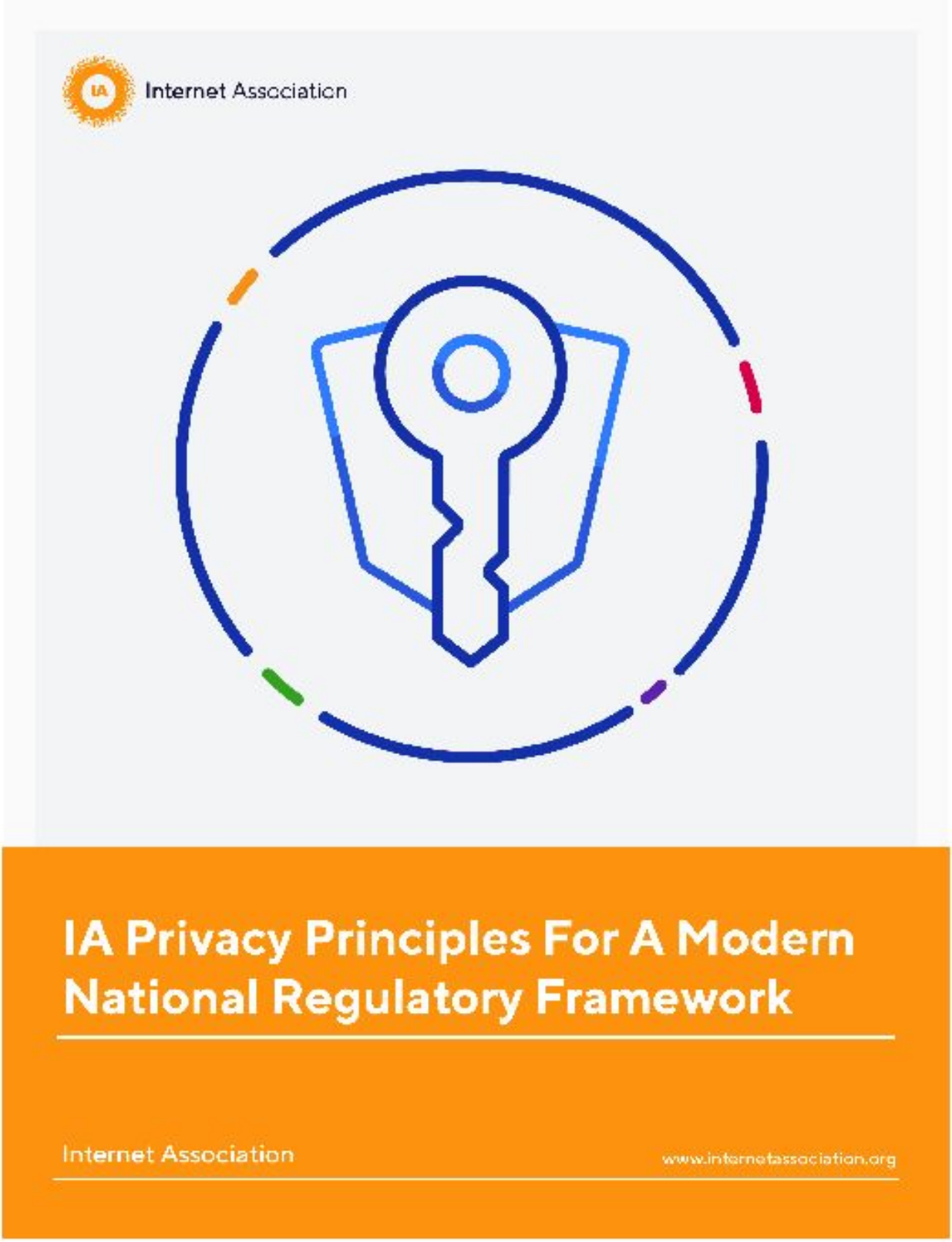
IA's privacy principles place a heavy emphasis on context as the basis for any new national privacy framework. This means that such a framework must be flexible, taking into account the reasonable expectations individuals have regarding how the personal information they provide companies will be used, the sensitivity of personal information they provide to companies, and the concrete risk to individuals of the potential misuse or unanticipated sharing of such personal information. This risk-based approach will protect consumers when they need it most and also recognize that data—even the same piece of information—can present different harms based on who has it and how it is being used.

To provide meaningful and comprehensive privacy protections, a federal privacy law must cover all parts of the economy and eliminate the risk that a confusing patchwork of state laws could impose conflicting obligations on companies that serve customers in multiple states. Americans should have consistent experiences and expectations across state lines and industries – regardless of whether they're interacting with a company online or offline.

Internet Association and our member companies stand ready to work with this Committee and all other interested parties on an American approach to protecting people's privacy that allows for continued U.S. leadership in technology. The time is now for a national privacy law that provides consumers in every state both on and offline meaningful control over data in all sectors of the economy. Our goal is to see bipartisan legislation signed by the president this year.

Sincerely,

Michael Beckerman
President and CEO


Internet Association
IA Privacy Principles For A Modern National Regulatory Framework
Internet Association
www.internetassociation.org

Introduction

The time is right to modernize our federal rules and develop a national framework for consumer privacy. That framework should be consistent nationwide, proportional, flexible, and should encourage companies to act as good stewards of the personal information provided to them by individuals.

As policymakers and stakeholders work on an updated approach to privacy, we must ensure that a national privacy framework:

- Protects individuals' personal information and fosters trust by enabling individuals to understand their rights regarding how their personal information is collected, used, and shared;
- Meets individuals' reasonable expectations with respect to how the personal information they provide companies is collected, used, and shared, and the context-dependent choices they have;
- Promotes innovation and economic growth, enabling online services to create jobs and support our economy;
- Demonstrates U.S. leadership in innovation and tech policy globally;
- Is mindful of the impact of regulation on small- and medium-sized companies; and
- Applies consistently across all entities to the extent they are not already regulated at the federal level.

Context For Principles

Our country's vibrant internet ecosystem provides individuals with unprecedented personal, social, professional, educational, and financial benefits, contributing an estimated 6 percent of U.S. GDP and nearly 3 million American jobs. The internet enables all levels of government and every sector of the economy to become more citizen- and consumer-centric by providing innovative tools, services, and information, and allowing for a more efficient use of resources.

IA companies believe trust is fundamental to their relationship with individuals. Our member companies know that to be successful they must meet individuals' reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and to continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, our member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

There are a range of strong privacy, data security, consumer protection, and anti-discrimination laws that exist today. These include Section 5 of the FTC Act and the Clayton Act, as well as more than 15 other federal statutes and implementing regulations that are sector specific or relate to particular activities.[2] Additionally, there are myriad state laws relating to privacy and data security, enforced by

[2] These are the Children's Online Privacy Protection Act ("COPPA") and the FTC's COPPA Rule; the Gramm-Leach-Bliley Act, and the FTC's Privacy and Safeguards Rules; the Electronic Fund Transfer Act; the Fair Credit Reporting Act; the Fair and Accurate Credit Transactions Act; the Equal Credit Opportunity Act; The Truth in Lending Act; the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act of 2003 and the FTC's CAN-SPAN Rule; the Telephone Consumer

state attorneys general or private litigants, including state data breach notification statutes and unfair and deceptive acts and practices statutes; data security and encryption laws; and a variety of other privacy laws that relate to online privacy, social security numbers, and data brokers. Our member companies comply with these current laws as well as with self-regulatory principles and rules that govern how they operate and do business.[3] However, this array of laws also creates a "patchwork" effect that complicate compliance efforts and lead to inconsistent experiences for individuals. A new, comprehensive national framework would create more consistent privacy protections that bolster consumers' privacy and ease compliance for companies.

This document sets forth: (1) principles for a national privacy framework, and (2) considerations for policymakers when evaluating such a national privacy framework.

Privacy Principles

These privacy principles aim to protect an individual's personal information, which we define as any information capable of identifying a specific individual or a device that belongs to that individual.

- **Transparency**. A national privacy framework should give individuals the ability to know whether and how personal information they provide to companies is used and shared with other entities, and if personal information is shared, the categories of entities with whom it is shared, and the purposes for which it is shared.
- **Controls**. Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, except where that information is necessary for the basic operation of the business or when doing so could lead to a violation of the law.
- **Access**. Individuals should have reasonable access to the personal information they provide to companies. Personal information may be processed, aggregated, and analyzed to enable companies to provide services to individuals. Safeguards should be included to ensure that giving an individual the ability to access their personal information does not unreasonably interfere with other individuals' privacy, safety, or security, or a company's business operations.
- **Correction**. Individuals should have the ability to correct the personal information they provide to companies, except where companies have a legitimate need or legal obligation to maintain it.
- **Deletion**: Individuals should have the ability to request the deletion of the personal information they provide to companies where that information is no longer necessary to provide the services, except where companies have a legitimate need or legal obligation to maintain it.
- **Portability**. Individuals should have the ability to obtain the personal information they have provided to one company and provide it to another company that provides a similar service for which the information is necessary.

The adoption of the principles identified above would enhance individuals' personal privacy and ensure

---

Protection Act; the Restore Online Shopper's Confidence Act; the Video Privacy Protection Act; the Cable Act; the Electronic Communications Privacy Act; the Computer Fraud and Abuse Act; the Stored Communications Act; the Telemarketing and Consumer Fraud and Abuse Prevention Act and the FTC's Telemarketing Sales Rule, including the Do Not Call Rule and Registry; and the U.S. Safe Web Act.

[3] These self-regulatory bodies have developed their own codes of conduct, including the Data and Marketing Associations Ethical Business Practices; the Network Advertising Initiative's 2018 Code of Conduct; the Digital Advertising Alliance's set of Self-Regulatory Principles relating to online advertising, which are enforced by the Accountability Program of the Council of Better Business Bureaus; and the Payment Security Industry Data Security Standards (PCI-DSS), for those that accept payment cards.

individuals' trust. To ensure the effectiveness of a national privacy framework, these principles must be balanced against: (1) competing individual rights, including freedom of speech and expression; (2) other parties' privacy interests; (3) data security interests; (4) companies' needs to protect against fraud or other unlawful activity, or individual safety; (5) companies' requirements to comply with valid law enforcement requests or judicial proceedings; (6) whether the exercise of the rights afforded individuals are unduly burdensome or excessive in specific instances; and (7) whether individuals' exercise of their rights would require companies to collect or process additional personal information about that individual.

Proposed Considerations for Policymakers

Fostering privacy and security innovation. A national framework should not prevent companies from designing and implementing internal systems and procedures that enhance the privacy of each individual's personal information. Companies should take into account privacy and data security when they design and update their services, for example, by de-identifying, pseudonymizing, or aggregating data.

A national data breach notification law. A national framework should specifically preempt the patchwork of different data breach notification laws in all 50 states and the District of Columbia to provide consistency for individuals and companies alike. This national standard should protect individuals and their personal information through clear notifications, define a harm-based trigger for notification to avoid notice fatigue, and allow companies flexibility in how they notify individuals of unauthorized access to their personal information.

Technology and sector neutrality. A national privacy framework should include protections that are consistent for individuals across products and services. Such a framework should be both technology neutral (no specific technology mandates) and sector neutral (applying to online and offline companies alike).

Performance standard based approach. A national privacy framework should focus on accomplishing privacy and data security protections, but laws and regulations should avoid a prescriptive approach to doing so, as such an approach may not be appropriate for all companies and may well become obsolete in light of rapidly developing technology.

Risk-based framework. A national privacy framework should be grounded in a risk-based approach, based on the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm for its misuse or unauthorized access. Consistent with FTC data security order provisions and the FTC's unfairness standard, companies should identify and address reasonably foreseeable risks to the privacy and the security of personal information where the result of failing to address the risk would cause, or be likely to cause, tangible consumer harm.

A modern and consistent national framework for individuals and companies. A national privacy framework should be consistent throughout all states, preempting state consumer privacy and data security laws. A strong national baseline creates clear rules for companies and ensures that individuals across the United States can expect consistent data protections from companies that hold their personal information. A national privacy framework should primarily be enforced by the FTC at the federal level and by state attorneys general at the state level, where the FTC declines to act.