Internet Association's Comments in Response to NTIA Request for Comments:
Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780–8780–01

INTRODUCTION

Internet Association ("IA") welcomes the opportunity to comment on the National Telecommunications and Information Administration's ("NTIA") Request for Comments on Developing the Administration's Approach to Consumer Privacy ("RFC"). IA's mission is to foster innovation, promote economic growth, and empower individuals through the free and open internet. IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.

NTIA's RFC demonstrates a thorough understanding of the complexities of consumer privacy and the need for a framework that is flexible, consumer friendly, and that enables innovation. The approach that NTIA has proposed—one that articulates outcomes rather than dictating how those outcomes should be achieved—appropriately balances the overall context in which a product or service operates against individuals' reasonable expectations about their privacy. In addition, the high-level goals that NTIA has articulated as federal priorities recognize the need for a harmonized approach that is comprehensive, scalable, and transparent.

IA recently released its own proposed framework: "IA Privacy Principles For A Modern National Regulatory Framework" ("IA Principles"). IA believes that its framework also demonstrates a commitment to consumer privacy while maintaining a regulatory environment that promotes innovation and fosters growth. We are pleased to see that many of the same concepts found in the IA Principles are echoed in NTIA's RFC.
Recent Senate Commerce Committee hearings on privacy legislation have demonstrated there is a wide consensus among industry, public interest organizations, regulators, and academics that the time for new, comprehensive federal privacy legislation is now. The current patchwork of state, federal, and international laws on data privacy and security imposes significant regulatory burdens on companies without achieving meaningful protections for individuals. Individuals are unclear on what their rights are, or how to meaningfully exercise them. Companies, particularly those that are smaller or more resource constrained, are likewise overburdened by having to comply with numerous laws, rules, and guidance in each of the 50 states and in jurisdictions around the world. IA believes that individuals need consistent and meaningful consumer privacy protections at the federal level, and that companies that collect personal information would also benefit from clarity on privacy rules.

IA therefore believes, consistent with NTIA, that it is critical that the United States take a leading position in consumer data privacy and security, and that this is best achieved by adopting a unified federal approach to most consumer privacy issues. IA believes that such an approach must:

- Provide the same protections for consumer data across most sectors, regardless of whether it is gathered offline or online, except for those sectors, such as financial services and healthcare, where there are existing federal laws that cover how personal information must be treated;
- Be established quickly to inform Congress, which is considering privacy legislation simultaneously with the NTIA's framework process;

- Be sufficiently detailed and clear, so that the standards will be easily understood by individuals and straightforward for companies of all sizes to implement; and
- Promote consistency by preempting state laws that seek to impose state-specific, and sometimes conflicting or different standards for the same conduct.

IA applauds NTIA for its focus on achieving meaningful outcomes for individuals, and for seeking to maximize data privacy and security through a flexible approach that allows small and medium-sized businesses ("SMBs") to grow and continue to innovate. We hope that following this RFC, NTIA will publish a final set of outcomes and goals, based on stakeholder input, that will support and advance the congressional work that lies ahead in developing a comprehensive federal privacy law.

Below please see IA's responses to the specific questions posed by the RFC.

FIRST SET OF REQUESTS FOR COMMENT: CORE PRIVACY OUTCOMES

A. THROUGH THIS RFC, THE DEPARTMENT IS FIRST SEEKING FEEDBACK ON WHAT IT BELIEVES ARE THE CORE PRIVACY OUTCOMES THAT CONSUMERS CAN EXPECT FROM ORGANIZATIONS.

1. Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?

The NTIA Privacy Outcomes cover many important elements of consumer privacy. IA recommends that NTIA include data portability as a privacy outcome.

Portability

IA believes that data portability, where appropriate, is also an important outcome for individuals and should be added to NTIA's list of Privacy Outcomes. IA's portability principle states: "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." Data portability allows individuals to take control of their data and exercise meaningful choice among service providers.

2. Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?

Outcome 1: Transparency

IA agrees with NTIA that transparency is a core privacy outcome, and has included it among IA's Principles. Specifically, IA's transparency principle states:

> 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.

We agree with NTIA that the Transparency outcome should be developed based on a performance standard, rather than a design standard. We further agree that the transparency outcome should focus on individuals being "able to easily understand how an organization collects, stores, uses, and shares their personal information," and that "organizations should...maximize the intuitiveness of how it [sic] conveys information to users."

IA believes that NTIA could provide useful guidance to lawmakers and regulators by providing examples of alternate means of achieving transparency for individuals other than through privacy statements. For example, just-in-time notices, dynamic user dashboards with contextual explanations and choice management functionality, and in-product settings are all mechanisms that provide transparency for individuals. These mechanisms continue to evolve, and will result in new ways of delivering important privacy information and choice to individuals.

Outcome 2: Control

IA agrees with NTIA that consumer control is an important outcome. However, we also believe that it should be context-driven. An individual's ability to exercise control over his or her personal data must be appropriately balanced against a company's legitimate interests so that it will not interfere with the ability to provide individuals with goods or services they request; conduct routine business operations; comply with laws or other legal obligations; or to protect other customers, networks, and third parties from harmful activity. For example, to prevent or investigate fraud, companies may need to prohibit individuals from immediately deleting their accounts and the associated personal information. Companies may also need to retain certain types of information to authenticate account owners before providing access to account data. In some cases, companies may need to limit the control options an individual has if they are subscribed to certain services. For example, a subscription service that offers recommendations and ratings to assist individuals in locating content of interest may not be available without the ability to use activity data.

In addition, context needs to be considered with regard to the mechanisms for consumers to exercise control. It may prove difficult for SMBs to make withdrawing consent "as readily accessible and usable" as the process of giving consent. For example, SMBs may not have the resources to develop advanced privacy centers or similar tools that can automatically implement changes to how data is used when individuals withdraw consent. Instead, these companies often rely on disclosures in their privacy policies that provide individuals with instructions on how to opt out of marketing or other data processing. Such companies then respond to individual requests via contact forms or email and efficiently make requested changes (whether to provide access to data, alter marketing preferences, or delete an entire account). In fact, many companies that have privacy centers, self-service dashboards, or in-product settings still receive communications from individuals who prefer to write directly to the company to make requests related to their data.

IA therefore proposes that NTIA recognize that there needs to be flexibility in how a control principle is described so that SMBs can achieve the objective of allowing individuals control, without having to build complicated and burdensome features into their products and services. As with any potential requirements that may be imposed, IA recommends the measures be adopted in a manner that embraces flexibility and context, and as frequently noted by the FTC in its orders and consent decrees, "be appropriate to the [company's] size and complexity, the nature and scope of [company's] activities, and the sensitivity of the personal information." [*See, e.g.*, FTC Decision and Order, In the Matter of Lenovo Inc., Docket No. C-4636, p. 6].

Outcome 5: Access and Correction

Another proposed core privacy outcome by NTIA is that, "[u]sers should have qualified access to personal data that they have provided, and to rectify, complete, amend, or delete this data." IA recommends that NTIA clarify

what "qualified access" means in this context. NTIA's Access and Correction outcome, as well as IA's access principle, recognize the importance of "reasonable" access as part of a national privacy framework. IA notes the importance of balancing consumer rights to access and correct personal data with a wide range of legitimate needs or obligations that the company holding the data may have. In addition, such rights of access should also not impinge on the rights of others, including privacy rights or other legal rights such as free expression, freedom of the press, and the right of access to information. To the extent that "qualified access" is meant to capture the concept that a right to access cannot be absolute and must be flexible, balanced with other interests, and context-based, IA agrees, and proposes that NTIA make that clear in its final framework.

Outcome 7: Accountability

IA supports a national, comprehensive data privacy and security law that includes accountability mechanisms for violations. Within a comprehensive statutory framework, there may be room for alternatives to regulatory enforcement that could help incentivize companies not only to comply with legal requirements, but to go beyond bare minimums and the status quo with innovative approaches to protect individuals' privacy interests. Safe harbors, third party certification programs, self-regulatory programs, and other mechanisms should be permitted to exist alongside regulatory enforcement so that regulators can focus their limited resources on truly important issues, and so that companies can continue to develop new and meaningful accountability approaches that benefit individuals. For example, in 2013 when the Federal Trade Commission ("FTC") updated the Rules for the Children's Online Privacy Protection Act, it included provisions for safe harbors with the hope of spurring innovation in mechanisms to verify age and obtain parental consent. *See* 16 C.F.R. Part 312. Similarly, following the FTC's 2009 Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, the Digital Advertising Alliance developed a series of principles that apply to the online advertising ecosystem and are monitored and enforced by an independent accountability program run by the Council of Better Business Bureaus.

To the extent that NTIA has other accountability mechanisms in mind, it would be helpful to further elaborate on the types of accountability mechanisms NTIA believes are consistent with achieving the other stated outcomes and how such mechanisms would work in practice.

3. Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?

As a general comment, IA agrees with the NTIA privacy outcomes and encourages NTIA to continue to provide detail on how these outcomes can be achieved in ways that also promote NTIA's stated goals: in particular, legal clarity while maintaining flexibility to innovate, a risk and outcome-based approach, and scalability.

For example, IA believes that the goals related to flexibility and scalability are particularly important with regard to the privacy outcomes discussed immediately below.

Outcome 2: Control

As stated earlier (*see infra* p. 3), NTIA's proposed Control outcome is broad and may be difficult to put into practice. IA believes that the description of this outcome should be more clearly balanced with a goal of allowing flexibility and avoiding unnecessary burdens on SMBs or a chilling impact on innovation, while maintaining the important privacy interests of individuals. Mostly importantly, IA respectfully proposes that

NTIA ensure that this concept is not so broad as to disrupt the ability of companies to provide the types of services that continually transform individuals' daily activities, personal and professional lives, and entertainment. It is appropriate to consider factors such as the context in which individuals share information with companies, the relationships individuals have with companies, individuals' reasonable expectations given the context of such relationships, the sensitivity of the data at issue, the level of engagement an entity has with such data, and the size and complexity of the entity itself. Such factors can be built into a flexible regime. For example, individuals should not be able to exercise complete control in a manner that limits use of their data and simultaneously expect that services that use that data to provide relevant content, products, or services will function in a manner that is consistent with the consumer's reasonable expectations. The control provision should also be limited to reflect and respect companies' right to make design decisions for their products and services. This can be achieved by more clearly articulating that control, like other privacy interests, should make sense within the context of the relationship between the individual and the business.

Outcome 3: Reasonable Minimization

IA believes that companies should carefully consider privacy as part of their design process, including an analysis of what data may be needed to provide a compelling consumer experience in connection with the specific goods or services. To develop innovative and engaging services, companies will need latitude to collect and use data that is appropriate to the context. Any guideline for data minimization needs to be flexible enough to allow organizations to consider what is appropriate given the potential sensitivity of the data and how it may be used. Companies may need to collect data beyond that strictly necessary to offer a service so that they may implement network security controls and anti-fraud measures; develop and use artificial intelligence and machine learning to improve their services; prevent illegal activity; identify violations of their terms of use or other potentially harmful manipulations of their networks; and to understand how their websites and mobile applications can be optimized based on analytics data.

Importantly, minimizing data can result in unintended discriminatory practices. For example, if companies do not collect and process enough of the right types of data for AI and machine learning, their AI applications may make discriminatory correlations based upon training sets that are too small or do not contain the most relevant data for the purpose. An example is the mobile app "Street Bump" that detected pot-holes in Boston using sensors in smartphones and then reported them to the department of public works; the app wound up systematically directing city services to wealthier neighborhoods where individuals were more likely to carry cellphones.

Minimization should be offered alongside security measures, aggregation/deidentification, and other existing and developing context-based techniques to protect individuals' personal information while permitting companies the room to move forward with innovative development. Given the need for flexibility and the difficulty of defining reasonableness in the context of different products and services, this may be an area that would benefit from the development of industry guidelines.

Outcome 4: Security

IA believes that any security outcome should be carefully articulated to allow companies that handle personal data to comply with requirements that are appropriate to their size, the nature of their interactions with personal data, and the sensitivity of the data itself. An approach that is flexible and carefully tailored to actual

risks that specific enterprises face is most consistent with the "Risk Management" privacy outcome NTIA describes. Security outcomes should be considered as part of a holistic view of the protection of information throughout an organization.

While IA appreciates NTIA's sentiment that companies should "meet or ideally exceed current consensus best practices," we fear that the aspirational nature of this statement could be misinterpreted to imply that that companies that meet best practice standards are not meeting security standards, or that companies that meet certain standards, but not others, based on informed judgments regarding the risks associated with their specific enterprise, may be out of compliance with this outcome. *See* 83 Fed. Reg. 486000, 486002 (Sept. 26, 2018). A new national framework or legal standard must be appropriately drafted to recognize that security is not a one-size-fits-all proposition.

Outcome 5: Access

IA reiterates its concern, stated in its own principles, that consumer access rights be subject to appropriate limitations in order to, among other things, protect the rights of others, including their privacy rights. Limitations may be appropriate to safeguard user account information from unauthorized attempts to obtain the data by pretending to be the authorized individual. Further, any right of access to data should be carefully limited to protect the identities of other individuals who may have submitted complaints to service providers, or to protect employees engaged in content review to protect such individuals from harassment. Rights to correction or deletion should not interfere with the reporting of news, the public's right to access information on topics of public interest, or the need for companies to maintain data, such as where there are allegations of sexual harassment. There are many legitimate reasons for individuals to seek access to their own account data, to seek corrections, or to request removal. To preserve legitimate exercises of these interests, there must be appropriate limitations to prevent abuses that interfere with reasonable needs to maintain certain data and to protect the privacy and other legitimate rights of others.

Outcome 7: Accountability

As explained above (*see supra* p. 4), IA agrees with the general proposition that accountability is a necessary component of a national framework for data privacy and security. While IA believes that Congress should act with urgency to draft a comprehensive legislative framework that includes regulatory enforcement, we are uncertain what type of accountability system NTIA has in mind. We think there is room to consider complementary frameworks, such as certifications, safe harbors, and self-regulatory frameworks with strong accountability mechanisms. IA also believes that NTIA's Accountability outcome needs further elaboration, that it must afford companies with due process, and that its place in an overall legislative framework should be more clearly explained. IA encourages NTIA to consider incentive-based accountability options alongside the more traditional, restrictive regulatory frameworks adopted elsewhere.

SECOND SET OF REQUESTS FOR COMMENT: HIGH-LEVEL GOALS

B. THE DEPARTMENT IS ALSO SEEKING FEEDBACK ON THE PROPOSED HIGH-LEVEL GOALS FOR AN END-STATE FOR U.S. CONSUMER- PRIVACY PROTECTIONS. [P.13]

1. Are there other goals that should be included, or outcomes that should be expanded upon?

IA believes that the following high-level goals are also essential to a national privacy framework:

Preemption

As stated in the IA Principles:

> [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 individuals across the United States can expect consistent data protections from companies and ensures individuals across the United States can expect consistent data protections from companies that hold their personal information.

IA believes that preemption of state consumer privacy and data security laws should be included as an explicit goal. As NTIA acknowledges in its harmonization goal, it is not to the benefit of individuals or industry for any further framework to be adopted that cannot effectively harmonize existing requirements and stop the proliferation of new, sometimes conflicting, obligations. Any effort that falls short of these goals will ultimately be unsuccessful in achieving the identified privacy outcomes or NTIA's stated goals, including comprehensive application, harmonization and interoperability. Moreover, a comprehensive and preemptive national privacy framework for the U.S. will help give the U.S. a "seat at the table" in efforts to achieve interoperability with other countries that have already adopted comprehensive privacy legislation. Finally, the nature of 21st century digital commerce renders the patchwork of state laws, many of which conflict with one another, nearly impossible to meaningfully implement. A preemptive federal framework would permit companies and individuals to gain both clarity and alignment on expectations for the relationship.

Flexibility

IA agrees with NTIA's stated goal that incorporating flexibility is an essential element to a successful privacy framework. (*See* 83 Fed. Reg. at 486002). To achieve maximum benefit for individuals and remain mindful of the impact on SMBs, IA believes that the privacy outcomes and goals must allow for flexibility in how the desired outcomes and goals are achieved. Flexibility—allowing for a performance standard rather than a design standard—will not only stimulate innovation in the delivery of privacy protections, but it will also avoid unnecessarily prescriptive rules being imposed on small enterprises without necessarily providing better privacy protection for individuals.

Tech and Sector Neutral

Only a comprehensive approach, harmonized with existing sector-specific laws, will provide a coherent and predictable set of expectations for individuals. IA believes that the focus should be on data practices rather than on the specific technology or sectors to enable the framework to evolve alongside business practices and technologies. In addition, technology neutrality is essential to avoid regulation standing in the way of innovation and to allowing legal standards to evolve with technology.

IA recognizes that some types of personal information may require special rules to ensure proper handling, and that in some instances federal sectoral privacy laws, like HIPAA, GLBA, and COPPA, already fill this need. For practices not already regulated at the federal level, IA believes that personal data should be subject to a single set of regulations regardless of the industry sector or whether the data is collected or stored online or offline. This dovetails with NTIA's goal of comprehensive application, because only a comprehensive approach will provide a coherent and predictable set of expectations for individuals.

2. Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described?

The RFC is ambiguous as to whether NTIA is aimed at developing best practices and principles or potential regulation. IA believes that the final NTIA principles should be clear that the Administration believes that they serve as a model for comprehensive federal privacy legislation.

NTIA further proposes incentivizing privacy research. IA would like to highlight that the government can play a vital role in promoting the overall area of privacy engineering, continuing to foster STEM and data science-focused educational programs to support the goals of the draft framework, and promoting the long-term growth and innovation of U.S. companies in the development of privacy- and security-enhancing technologies.

3. Are there any risks that accompany the list of goals, or the general approach taken by the Department?

With regard to NTIA's statement in its Accountability outcome that "there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations," IA believes this principle should be context-based and informed by the size of the organization, the nature of an organization's interaction with personal information, the nature and sensitivity of the data, and who ultimately has responsibility for any failure to properly handle the data. To this end, examples in the final framework would be helpful to individuals and industry alike.

THIRD SET OF REQUESTS FOR COMMENT: NEXT STEPS

C. The Department is seeking comments that describe what the next steps and measures the Administration should take to effectuate the previously discussed user-centric privacy outcomes, and to achieve an end-state in line with the high-level goals. In particular:

1. Are there any aspects of this approach that could be implemented or enhanced through Executive action, for example, through procurement? Are there any non-regulatory actions that could be undertaken? If so, what actions should the Executive branch take?

IA recommends NTIA publish a refined set of outcomes and goals, based on stakeholder input, that will support and advance the significant work that lies ahead in developing a comprehensive federal privacy law.

2. Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?

IA believes that NTIA should encourage stakeholder participation in discussions about areas that are unlikely to be addressed by consumer-focused federal data privacy and security legislation, such as priorities for incentivizing privacy research and mechanisms for international interoperability. IA also believes that NTIA should invite further discussion on difficult issues where delicate balances must be struck, for example, how to balance consumer interests in data access and correction while ensuring companies are able to protect other individuals, their networks and services, and the public.

3. What aspects of the Department's proposed approach to consumer privacy, if any, are best achieved

via other means? Are there any recommended statutory changes?
Congress is working on federal privacy legislation, and IA believes that Congress should use NTIA's self-regulatory framework, when final, to inform the process. As Congress is moving quickly with hearings on such legislation, IA believes that NTIA should also move quickly to finalize its approach, so that it may be used as a meaningful guide for congressional deliberations.

FOURTH SET OF REQUESTS FOR COMMENT: KEY TERMS

D. THE DEPARTMENT UNDERSTANDS THAT SOME OF THE MOST IMPORTANT WORK IN ESTABLISHING PRIVACY PROTECTIONS LIES WITHIN THE DEFINITIONS OF KEY TERMS, AND SEEKS COMMENTS ON THE DEFINITIONS. IN PARTICULAR:

1. Do any terms used in this document require more precise definitions?
IA believes that the following terms require more precise definitions: "Personal information"; "Qualified Access"; "Reasonable Minimization"; "Accountability."

2. Are there suggestions on how to better define these terms?
Personal Information
In its own principles, IA has defined "personal information" as "any information capable of identifying a specific individual or a device that belongs to that individual," which is consistent with the definition adopted by the Asia-Pacific Economic Cooperation Privacy Framework.

Qualified Access
IA believes that "qualified access" should mean that a right to access cannot be absolute and must be flexible, balanced with other interests, and be context-based.

Reasonable Minimization
IA believes that "reasonable minimization" should be defined in a way that is not absolute and that allows organizations to consider what "minimization" is appropriate given the potential sensitivity of the data and how it may be used. In addition, reasonable minimization should reflect that there are existing and developing context-based techniques to protect individual information while permitting companies the room to move forward with innovative development.

Accountability
IA believes that accountability can take multiple forms, such as safe harbors, third party certification programs, self-regulatory programs, and other mechanisms that provide meaningful oversight to businesses while affording them due process in any accountability action.

FIFTH SET OF REQUESTS FOR COMMENT: FTC AUTHORITY

E. ONE OF THE HIGH-LEVEL END-STATE GOALS IS FOR THE FTC TO CONTINUE AS THE FEDERAL CONSUMER PRIVACY ENFORCEMENT AGENCY, OUTSIDE OF SECTORAL EXCEPTIONS BEYOND THE FTC'S JURISDICTION. IN ORDER TO ACHIEVE THE GOALS LAID OUT IN THIS RFC, WOULD CHANGES NEED TO BE MADE WITH REGARD TO THE FTC'S RESOURCES, PROCESSES, AND/OR STATUTORY AUTHORITY?

The FTC is the appropriate agency to enforce consumer-focused data privacy and security laws. The FTC has demonstrated a vigorous approach to enforcement activity for two decades that achieves both immediate and longer-term goals, by stopping inappropriate handling of consumer data; requiring companies to commit to plans designed to ensure data handling will be legally compliant in the future; and providing guidance on achieving regulatory compliance in areas where existing standards may be unclear.

There is no doubt that there are resources that could enhance the FTC's ability to conduct meaningful enforcement of existing privacy laws and any new comprehensive data privacy and security regime that may include newly covered entities, data types, and regulatory obligations. In addition, the FTC has always embraced a mission of educating individuals on their rights and protections under the law, and this effort should be encouraged and appropriately resourced. The FTC also educates organizations on their obligations and best practices, such as the recently launched Cybersecurity for Small Business campaign. IA further believes that the FTC and the state attorneys general have worked well together in law enforcement and education efforts.

The FTC has said that it believes that it needs APA rulemaking authority and civil penalty authority as part of a new federal law. IA believes that it is premature to conclude that rulemaking and civil penalty authority is necessary for a law that has yet to be drafted, let alone enacted.

SIXTH SET OF REQUESTS FOR COMMENT: REPLICATION GLOBALLY

G. IF ALL OR SOME OF THE OUTCOMES OR HIGH-LEVEL GOALS DESCRIBED IN THIS RFC WERE REPLICATED BY OTHER COUNTRIES, DO YOU BELIEVE IT WOULD BE EASIER FOR U.S. COMPANIES TO PROVIDE GOODS AND SERVICES IN THOSE COUNTRIES?

IA believes the answer is "yes," especially with respect to the goals of interoperability and scalability, together with flexibility in achieving NTIA's proposed outcomes. A harmonized global approach with these principles would afford individuals with meaningful privacy protections while providing a much more practicable, performance-based regime for companies than, for example, the code-based, design standard outlined in the GDPR. A key component to promote such an approach would be for the U.S. to join the community of nations around the world that have already enacted comprehensive national privacy laws, while learning from the opacity and inflexibility of some of those laws.

SEVENTH SET OF REQUESTS FOR COMMENT: U.S. LEADERSHIP

F. ARE THERE OTHER WAYS TO ACHIEVE U.S. LEADERSHIP THAT ARE NOT INCLUDED IN THIS RFC, OR ANY OUTCOMES OR HIGH-LEVEL GOALS IN THIS DOCUMENT THAT WOULD BE DETRIMENTAL TO ACHIEVING THE GOAL OF ACHIEVING U.S. LEADERSHIP? [P.14]

Please see IA's response to NTIA's Sixth Set of Requests for Comment: Replication immediately above.

CONCLUSION

We look forward to continuing to work with constructively with NTIA in developing its final framework.

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-dependant 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.[1] Additionally, there are myriad state laws relating to privacy and data security, enforced by 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.[2] 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.

1. 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 analysed 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 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.

2. 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).

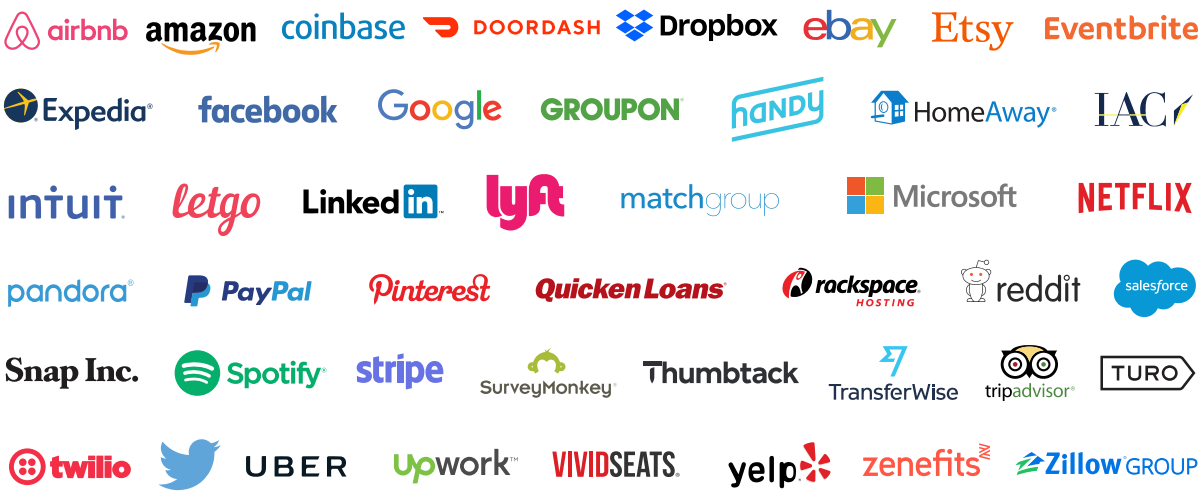
Performance standard based approach. A national privacy framework should focus on accomplishing privacy and data security protections, but laws and regulations should avoid a prescriptive approach to doing so, as such an approach may not be appropriate for all companies and may well become obsolete in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

1 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 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.

2 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.



The unified voice of the internet economy

www.internetassociation.org

Internet Association 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 as the voice of the world's leading internet companies, Internet Association works to ensure legislators, consumers, and other stakeholders understand these benefits.