ESPC
Email Sender & Provider Coalition

November 7, 2016

Via electronic mail to privacyrfc2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

RE: Request for Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

To Whom it May Concern:

The Email Sender and Provider Coalition ("ESPC") hereby submits its comments in response to the National Telecommunications and Information Administration's Request for Comments ("RFC") on the framework it proposes for Developing the Administration's Approach to Consumer Privacy ("Framework").

Formed in 2002, the ESPC is an industry association representing many of the largest technology providers in the email industry, including Email Service Providers ("ESPs"), Mail Transfer Agents ("MTAs"), application and solution developers and deliverability solution providers. The ESPC's 43 members assist in delivering a significant proportion of email for a large portion of America's most well-known brands.

The ESPC's mission is to advocate on behalf of email senders, providers, and other digital marketers operating globally in the online, mobile, and social media environments in favor of global laws and self-regulatory efforts that balance consumer protection and business innovation; to educate its membership on current and emerging business and legal developments affecting its membership; and to continue to develop and refine best practices that foster innovation, industry growth, and consumer trust. ESPC member companies are directly affected by data privacy and security laws and regulations, but in most instances do not have a direct relationship with the consumer. We would like to share our comments on the proposed Framework from this unique perspective.

We agree with many of the goals and aims outlined in the Framework. Specifically, we would like to highlight the importance of considering the impact of any new obligations on small and medium-sized businesses; making the Framework technology neutral and, to the extent possible, sector-neutral; and harmonizing the existing regulatory environment to reduce compliance costs and to promote meaningful privacy and security outcomes for consumers.

As discussions about federal legislation progress, NTIA can play an important role by elaborating on the Framework, as we have proposed below, but also by taking into account the comments of a wide variety of stakeholders and allowing companies in various industries to develop self-regulatory programs or codes of conduct that apply the final Framework to their industries so that the Framework can be easily understood and incorporated by the myriad types of businesses to which the Framework will apply into their own products, services, and consumer experiences.

Please see below our comments on many of the specific questions posed.

FIRST SET OF REQUESTS FOR COMMENT: CORE PRIVACY OUTCOMES

A. **Through this RFC, the Department is 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 ESPC does not believe that there are any additional outcomes that are necessary beyond those stated in the RFC, as we have commented on them below: Transparency; Control; Reasonable Minimization; Security; Access and Correction; Risk Management, and Accountability.

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

Transparency: The ESPC agrees that transparency with consumers is an important principle that should be part of any data privacy and security framework. That said, we think that it would be very helpful if the Department could provide several illustrative examples to allow organizations of all sizes and with all types of relationships with consumers to easily understand how they can achieve the Transparency outcome in the final Framework.

Control: Many ESPC members have built consumer-facing controls, for example a "privacy center" or other settings menu, that allow consumers to exercise control over their personal information and their marketing preferences. While these organizations have been able to achieve a mechanism for consumer control that is easy to use and can quickly achieve the consumer's goal, not every organization is able, nor should they be required, to build this type of mechanism. The RFC provides that "controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity." 83 Fed. Reg. 48600, 48601 (September 26, 2018). It is difficult to implement this general principle in practice, where consumers' experiences vary widely. Accordingly, the ESPC suggests a more flexible approach to the Control privacy outcome explicitly recognizing that: (1) in some contexts there may be limited "options" available for consumers to exercise control and as long as mechanisms are easy to find and effective, that is sufficient; and (2) requirements should be "appropriate to the [organization's] size and complexity; the nature and scope of the [organization's] activities …and the sensitivity of the [personal] information," as the FTC recognizes in the context of required security measures in its orders and consent decrees. In addition, it is important to recognize that in certain instances an organization may not be the appropriate entity to take the requested action, or an organization may not be able to accommodate the consumer's request because the information is essential to the basic operation of the business, subject to legal or regulatory requirements, or important to exercise a right or to protect other consumers, the organization, or the public.

Access: The Department states, "Users should have qualified access to personal data that they have provided, and to rectify, complete, amend, or delete this data." 83 Fed. Reg. 48600, 48602 (September 26, 2018). It would be helpful if the Department could elaborate on what is meant by "qualified access." The ESPC appreciates that the draft Framework elaborates on certain limitations that should apply to this access, such as the access should not interfere with an organization's legal obligations or the ability of third parties to exercise other rights provided by law. However, these limitations seem to suggest that the consumer's ability to access, rectify, complete, amend or delete their personal data make sense in all contexts. The ESPC proposes that this ability should only be required where it specifically furthers a consumer's privacy protections. For example, if a consumer chose to complete only the required fields when registering an online account, should the organization be required to build a system to allow the consumer to provide the organization with *more* personal information later, even though it is not required to offer or improve the service? In other instances, requiring amendment or rectification could require significant effort by an organization without any countervailing risk of harm to the consumer caused by potentially outdated or inaccurate information. For example, if an adult user made an error when inputting his or her data of birth into a system to confirm that he or she is over 13 and not subject to COPPA, and the provider only used that information to establish that the individual is an adult, should the provider be required to allow the consumer to change the day of month for sake of correctness? The Department should make clear that the Access outcome allowing consumers to rectify, complete, or amend is appropriate at least in part based on the risk of harm to the consumer that can be addressed through such actions. In other words, there should be some value that is achieved through the exercise of such a set of rights.

In addition, the ESPC believes that the Access outcome should clarify that consumers should in all cases direct their access requests to the organization that collected their information and with whom they have a relationship, rather than having a right to access their personal information from the service providers of such organizations.

Accountability: It is not clear what the Department intends by the phrase "external accountability." ESPC believes that an accountability program similar to the Council of Better Business Bureaus for online interest-based advertising is a good framework in this context. We also note that the Department has addressed the allocation of responsibility for responsible data practices between the "controller" and the "processor." Data controllers can be expected to take reasonable steps to require third-party service providers to handle personal data responsibly and in accordance with any legal restrictions or protections that may apply, and to make reasonable inquiries into whether the processor is able to fulfill these responsibilities. In practice, however, it is impossible for controllers to "ensure" third-party accountability. The ultimate framework adopted by the Department should clearly outline how the Accountability outcome applies to organizations depending on their relationship with the consumer and the personal data at issue.

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

Controls: As elaborated on above, organizations may take many different approaches to giving users control over their personal information. The divergence in methods of control is well-founded based on differences in technical capability, sophistication of the enterprise, the nature of the product, and what is practicable to attain the goal for the consumer. As NTIA framed the outcome, it is too general to put into practice. We further believe that it needs to be more flexible to recognize that user control interests must be balanced against reasonable needs a business may have to deliver services that the consumer has requested, such as keeping track of the open rates of emails consumers request and that ESPs send on their behalf. A failure of a consumer to open a company's emails over an extended period of time indicates a disengagement with the brand, which may cause the brand to ask the consumer if he or she still wants to receive opt-in emails.

Data Minimization: The ESPC agrees that organizations should give careful consideration to what information they need to collect from consumers in order to offer their products and services. In many instances, organizations can limit collection of personal information to only essential elements and still offer the service as designed. In other, more elaborate, systems, the concept of need should be thought of more broadly and should include consideration of what may aid network security, fraud prevention, anti-abuse measures, and other measures that provide a value to the consumer as well as the larger ecosystem of the service at issue. In all cases, data minimization needs to be explicitly limited by legal obligations an organization may have to retain data, whether due to litigation, investigations, or regulatory requirements.

Security: The security outcome should reflect the considerations adopted by the FTC in its security decisions and orders, that security measures should be "appropriate to [the organization's] size and complexity, the nature and scope of [organization's] activities…and the sensitivity of the …personal information." (*See, e.g.*, FTC Decision and Order, *In the Matter of Blu Products, Inc.*, Docket No. C-4657, P. 4). As such, the aspiration that the NTIA expresses in the security outcome that organizations "should meet or ideally exceed current consensus best practices," may not make sense as it does not consider the FTC factors and therefore may impose unduly high security standards on small and medium-sized businesses. *See* 83 Federal Register No. 187, 486000, 486002 (Wednesday, September 26, 2018). We also note that the term "best practices" is itself aspirational. We urge NTIA to carefully consider the incentives to organizations to coalesce around consensus practices to ensure that they do not accidentally convert "best practice efforts" into "efforts to identify minimum requirements" by punishing groups that aim high in their self-regulatory efforts.

Access: Access rights are similar to the concept of user controls. As we have explained, there are potential risks of unnecessary burden to small and medium-sized organizations and of interference with business operations for organizations of all sizes. The Access outcome should more clearly reflect that the consumer interest in access should be in relation to the value that can be achieved through access. Consumer interests should be at their strongest when the consumer benefits significantly through having access and organizations would only be able to overcome such interests by pointing to a direct conflict with legal or business obligations, the safety of any person, the exercise of rights by another person, or other legitimate objective (including avoiding unduly burdensome or abusive requests).

Accountability: As the Accountability outcome is drafted, it is unclear to whom organizations would be accountable and how the accountability process would work in practice. To ensure an effective framework that appropriately balances the interests of parties involved, any accountability body should allow organizations under investigation an opportunity to respond to concerns before the body makes any determination public.

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.

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

Preemption: NTIA should work towards creating a framework that can act as starting point for comprehensive federal data security and privacy legislation preempting state breach notification,

62 Portland Road, Suite 44, Kennebunk, ME 04043 - P 207.467.3500 - Fax 207.985.2523

consumer privacy, and substantive state security requirements. Consumers and organizations will both benefit from a uniform set of standards.

Flexible: The ESPC urges the NTIA to be mindful of the impact of its final Framework on small and mid-sized organizations and should embrace flexibility as a way to ensure such organizations are not unreasonably burdened.

Neutral: To the extent possible, ESPC encourages the NTIA to adopt technology neutral and sector neutral language to be able to cover a wide range of entities and practices as technology evolves, new services are offered, and new businesses enter the market. The Framework should address personal information protection whether offline or online, as the consumer's interests in security, control, and access are the same in each instance. It may make sense to leave existing sector laws in place for the protection of sensitive information, such as children's information, health data, or financial data and such laws can be specifically excepted from the scope of a framework.

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

The terminology NTIA has chosen to use moves between discussion of best practices and regulation. It would be helpful if the Department could be more consistent in expressing what it would like to achieve with the final Framework. The ESPC believes that the appropriate focus for the Department is to develop best practice guidance that can be a foundation for eventual federal legislation.

Further, the ESPC believes that the final Principles should allow flexibility, taking into account the many different types of markets and consumer experiences to which the Principles will apply, so that business can understand and incorporate them into their products and services. For that reason, we support self-regulatory efforts and codes of practice developed by various industry coalitions to apply the final principles to their own industries.

ESPC also believes that the high-level goal of Interoperability should expressly recognize transfers of personal data from the European Union to the United States, and provide as an express goal that the Principles are designed to allow for such transfers.

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

With respect to "clear statutory authority" of the FTC for enforcement, this should not include APA rulemaking authority because Section 18 of the FTC Act allows the FTC civil penalties for violations of trade regulation rules of over $40,000 per incident. Thus, for example, a data breach involving 50,000 consumer credentials could result in civil penalties over $200 million, potentially dwarfing the fines available under Europe's General Data Protection Regulation ("GDPR"), and give the FTC far too much power to force settlements in light of civil penalties.

We also note that the Department has distinguished between "controllers" and "third-party vendors." ESPC recommends that the Department be clear about what obligations it believes organizations should bear depending on their relationship to the personal information and the consumer involved in a given data practice.

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?

ESPC recommends that the Department develop its final Framework with more detail and clarity, with examples as appropriate, and seek further comment by all interested stakeholders.

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?

The ESPC recommends that the Department convene a group to provide input to the best practices effort and to help avoid the potential risks that we have identified above. In addition, any further review of privacy-related issues should include a cost-benefit analysis, so that there is hard data on the costs to implement any new proposals and the corresponding benefits to consumers.

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?

Ultimately, consumers and organizations will benefit from the clarity and uniformity of having comprehensive federal privacy and security laws. Congress is working towards this goal. The Department should continue to develop and refine its approach so the framework it produces can inform the legislative process because, ultimately, federal standards for privacy are best achieved by legislation, informed by NTIA's final Framework. Further, the ESPC believes that self-regulatory efforts and codes of practice, developed by various industries to address their unique issues, but consistent with the final Principles, would help businesses of all types incorporate the Principles into their products, services, and consumer experiences.

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?

ESPC believes the following terms should be more precisely defined: "personal information," "qualified access," "accountability," and "controller," with an eye toward the high-level goal of Interoperability.

2. Are there suggestions on how to better define these terms?

ESPC believes that the group that the Department convenes for input on the Framework should work toward consensus definitions or explanations of these terms.

3. Are there other terms that would benefit from more precise definitions?

ESPC does not believe that any other terms in the draft Framework need more precise definitions, though we do think that self-regulatory efforts and codes of conduct developed by various industries, may flesh out certain terms for application to that industry, consistent with the final Framework.

4. What should those definitions be?

N/A

FIFTH SET OF REQUESTS FOR COMMENT: FTC AUTHORITY

E. <u>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</u>?

The FTC has shown itself to be an effective regulator in consumer privacy with its current statutory authority, and we recommend that there are no changes to its authority. If the FTC were given rulemaking or civil penalty authority, it would provide the FTC with too much power and leverage in investigations and negotiations given the civil penalties that would make the GDPR's fines look like a traffic ticket.

<u>SIXTH SET OF REQUESTS FOR COMMENT: REPLICATION GLOBALLY</u>

F. <u>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</u>?

The answer is undoubtedly "yes." Organizations are not just burdened by varying legal standards among the U.S. states, but also on an international scale. The expense and complexity of complying can be overwhelming for some organizations, such that they may be discouraged from growing their businesses and engaging in global commerce. A harmonized global approach, incorporating the goals of Interoperability and Flexibility in achieving outcomes, would afford individuals with meaningful privacy protections while minimizing complexity, risks of non-compliance, and the impact of overly prescriptive requirements (like those in the GDPR).

<u>SEVENTH SET OF REQUESTS FOR COMMENT: U.S. LEADERSHIP</u>

G. <u>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</u>?

As we have said earlier in our comments, ultimately, consumers and organizations will benefit from the clarity and uniformity of having comprehensive federal privacy and security laws. If the Department can finalize a Framework that successfully incorporates this RFC's focus on consumer privacy outcomes as well as goals for flexibility and mindfulness regarding impact on small and medium-sized businesses, the resulting Framework can be the basis for federal preemptive legislation that would achieve U.S. leadership. This will facilitate Interoperability and continue to fuel growth and innovation for U.S. businesses.

Respectfully submitted,

Dennis Dayman
Chairman, Board of Directors,
Email Sender and Provider Coalition