November 9, 2018

The Honorable David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
1401 Constitution Ave NW
Washington, District of Columbia 20230

RE: *Comments of ACT | The App Association to NTIA on* Developing the Administration's Approach to Consumer Privacy *[Docket No. 180821780–8780–01]*

Dear Assistant Secretary Redl,

ACT | The App Association submits these comments in response to the U.S. Department of Commerce National Telecommunications and Information Administration's (NTIA) request for comment (RFC) regarding the Administration's approach to consumer privacy.[1] We note that this RFC, and NTIA's work in the privacy space, is timely, and the App Association appreciates the opportunity to provide commentary in response to the questions presented.

I. Statement of Interest and General Views on the Administration's Approach to Consumer Privacy

The App Association represents more than 5,000 small to mid-sized mobile software and connected device companies in a $950 billion industry that supports 4.7 million jobs in the United States. App Association members lead America's next industrial revolution, transforming traditional industry sectors and government functions from healthcare and public safety to manufacturing and municipal government into dynamic, data-driven, and mobile enterprises. Today, the "tech sector" no longer exists as a separate, unique vertical. Rather, it has expanded and taken root as part of other industries, and in the process, it has been democratized into a startup economy that thrives across the nation, mostly outside of Silicon Valley. As cars begin to drive themselves and physicians adopt clinical decision tools that utilize artificial intelligence (AI), the United States is fast evolving into a "tech economy."[2] Moreover, companies thought of as tech heavyweights often have more in common with traditional economy players from a business model standpoint: the former just happens to use newer technologies and find ways to make them useful for people.

[1] Fed. Reg. Doc. 2018-20941 (filed Sept. 25, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf (RFC).

[2] Reed, Morgan, *There is no "tech industry,"* ACT | The App Association blog (Oct. 24, 2017).

The App Association serves as a leading resource for thought leadership and education for the American small business technology developer community in the privacy space. We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and useable guidance to ease the burden of compliance.[3] Further, we are committed to promoting proactive approaches to ensuring end-user privacy and note our endorsement of NTIA's support for privacy-by-design approaches.[4]

As regulators from across key markets abroad continue to rush to utilize approaches to regulation of the digital economy which are often heavy-handed, the United States has remained the greatest market in the world for building a startup due to its evidence-based and light-touch approach to regulating new industries. Across the world, other governments struggle to incent and sustain the digital economy growth seen only in this country because companies elsewhere often face great barriers to bringing novel products and services to market—slowing technological innovations to the pace of government approval.

Yet, the American approach to privacy is a work in progress, and the App Association agrees that the time for changes to the U.S. approach to privacy regulation has arrived. Federal sector-specific regulation of privacy, along with a patchwork of state-level laws and regulations, presents a very challenging scenario for a small business innovator. The App Association is supportive of a new federal privacy framework that will clarify the obligations of our members and generally urges that the U.S. approach to privacy to provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation.

As the RFC points out, reports of data security breaches and companies' misuse of personal data have caused a significant proportion of Americans to refrain from engaging in certain types of online activity.[5] We agree with NTIA that users must "trust that organizations will respect their interests, understand what is happening with their personal data, and decide whether they are comfortable with this exchange."[6] Trust is the linchpin of App Association members' economic viability. Even as more and more of our member companies take advantage of opportunities in the enterprise space, trust is just as—if not more—important as it is for companies that serve consumers directly.

---

[3] *See, e.g.*, ACT | The App Association, *General Data Protection Regulation Guide* (May 2018), *available at* https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf.

[4] RFC at 48602.

[5] RFC at 48600.

[6] *Id.*

II. Responses of ACT | The App Association to Specific Questions Raised in the Administration's Request for Comment

Below, we offer responses to various outcomes and high-level goals NTIA raises in its RFC:

A. Core Privacy Outcomes

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

As an initial matter, we agree that privacy outcomes ought to be expressed separately from any proposed policy framework. In some cases, regulation is the best method of achieving a given outcome, but consistent with most commonly accepted theories of regulation, governmental intervention is only appropriate where the value of the intervention to consumers, the government, companies, and the economy outweighs not intervening. We, therefore, appreciate that the RFC refrains from concluding that any desired outcome is necessarily best reached via regulation. Secondly, the App Association applauds the NTIA for identifying what appear to be carefully considered outcomes. For example, NTIA's RFC lists transparency first, noting that:

> [o]rganizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service does not lead to adequate understanding. Organizations should use approaches that move beyond this paradigm when appropriate.[7]

The App Association generally agrees with this description of how companies should approach transparency. Certainly, "lengthy notices" often fail to accomplish their purposes from consumers' perspective. In fact, a privacy policy on its own is only sufficient where "approaches that move beyond this paradigm" (such as just-in-time notices) are not the most appropriate modality. So long as they are truthful, privacy policies generally tend to serve the purpose of compliance under current law. But when putting resources toward compliance is mutually exclusive with serving users' or clients' interests, policymakers should rethink a law or regulation.

[7] RFC at 48601.

In general, we urge the NTIA to adopt its proposed outcomes as they are drafted. However, NTIA should collapse "Control" and "Access and Correction" into a single outcome. The twin concepts of "access" and "correction" are arguably corollaries to the ability to "control" whether and how a company collects data as well as what is done with that data. "Access" is in many cases a necessary condition for meaningful control of one's own data when held by a company. This consideration may seem semantic or trivial; however, the more outcomes are separated analytically, the more likely small business operators are to think of "privacy" as a separate, exogenous set of desired outcomes, divorced from the design or function of a product or service or its success in the market. To support an environment in which companies approach privacy as integral to users' or clients' experiences (and build it in, by design), government should strive to keep identification of desired outcomes streamlined and connected with one another where appropriate.

B. High-Level Goals for U.S. Consumer Privacy Protections

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

We applaud NTIA for laying out a thoughtful and thorough set of goals for federal action in the RFC. In response to this question, we offer a few considerations:

i. Interoperability with foreign laws is important and the App Association is generally supportive of the interoperability principles that appear in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System. The APEC CBPR concepts are important as the United States and EU conduct a review of their respective privacy laws. However, as NTIA notes, the United States leads the world in privacy enforcement and we urge policymakers not to think of the United States as trying to "keep up" with more detailed and prescriptive privacy approaches foreign governments—like the European Commission—have chosen to take. Just because a government's regulations are more detailed and prescriptive does not automatically mean that framework is better at protecting privacy. Simply put, the United States has produced a successful tech-driven economy by maintaining a more flexible approach with strong enforcement and—while the General Data Protection Regulation has merits and establishes important rights for EU data subjects—policymakers should not adopt the European approach as written.

ii. The App Association is especially supportive of NTIA's suggestion for federal action to include "harmoniz[ing] the regulatory landscape," "incentiviz[ing] privacy research," and ensuring that there is "FTC enforcement." Harmonizing the regulatory landscape is perhaps the most important aspect of any potential federal action on privacy. With the enactment of the California Consumer Privacy Protection Act, and several other states considering privacy legislation, a federal bill that does not preempt states would simply add another regulatory layer onto an already complicated patchwork of privacy rules.

    Vesting enforcement authority in the Federal Trade Commission (FTC) is also an important aspect of federal privacy policy. The FTC has been the leading privacy enforcer in the United States for several decades and has developed unique expertise in pursuing cases involving complex privacy issues raised by platforms and other online services employing high-tech features, but which arguably fail to adequately or accurately inform consumers.

    Although the FTC's approach benefits in many ways from its tendency to enter consent orders—allowing for a customized set of remedies that are tailored to specific cases—these orders sometimes fall short of a meaningful roadmap for lawful behavior to other market actors because they do not bind the Commission or the private sector with respect to activities not covered in the order itself.

    Therefore, we support Congress authorizing additional resources for the FTC so that it can pursue more cases on the merits to develop a more robust body of enforceable privacy law in federal courts.

iii. Privacy research is a crucial component of sound federal privacy policy. Emerging methods of providing products and services that use large amounts of data demand creative experimentation with privacy models. Meanwhile, privacy experts often employ a hypothetical or normative view of how consumers *should* behave when presented with privacy choices—or a lack of privacy choices—connected to the services or products with which they are interacting at a given moment.

We believe this theoretical approach is employed too often and that empirical evidence would go some way toward ameliorating policy outcomes that otherwise suffer from being based on theoretical or aspirational assumptions. For example, NTIA in 2013 led a multistakeholder process to develop a voluntary code of conduct for mobile apps to clearly and concisely communicate how apps collect and use consumer data. The forum was convened pursuant to a White House "Privacy Blueprint," directing the U.S. Department of Commerce to gather stakeholders to build consensus around various aspects of consumer privacy.[8] After the privacy experts participating in the process approved a final code of conduct, the App Association developed user interfaces and reported on consumer testing of some visual representations of what the short form notice code of conduct would require.

Unfortunately, despite a streamlined user interface and simple representations of privacy concepts, consumers were still often confused about who was collecting their data, with whom it was being shared, and why it was being collected, used, or shared. This is perhaps an inevitable outcome of a theoretical approach to privacy that is geared more toward compliance with a code of conduct or set of regulations than consumers' actual expectations given the unique contexts in which they find themselves at a given time and interacting with a given product or service. The findings also underscore that dynamic communication modalities between companies and consumers that go beyond the text of a privacy policy are usually necessary and preferred over static descriptions of data collection and processing. In sum, we support NTIA's suggestion to provide resources for privacy research to explore actual expectations and behavior in light of mutable factors like context—which tends to affect expectations.

C. Next Steps to Achieve an End-State

3. Are there any recommended statutory changes?

Yes, the App Association notes that in order to achieve regulatory harmonization in the United States, federal statute must be amended to preempt state laws. Moreover, a federal privacy framework should clarify the FTC's authority to prohibit unfair or deceptive privacy practices. For example, although the FTC could issue

[8] https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-applicationtransparency.

guidance under its current statutory authority as to how companies should allow users to access and control the use of their data, explicit statutory authority to require reasonable access and control would produce more potent results. Similarly, although the FTC's enforcement of its organic statute authorizing it to prevent unfair or deceptive acts or practices in commerce has targeted failures to adequately notify consumers truthfully of a company's privacy practices, no statutory transparency requirement currently exists. Therefore, legislation could include a requirement that companies provide reasonable notice—which necessarily must be a flexible concept given context, consumer expectations, etc.—to consumers as to the types of information collected, what the information is used for, with whom it is shared, and why it is collected, used, and shared.

E. Changes to the FTC's Resources, Processes, and/or Statutory Authority

We acknowledge that every government agency must operate with resource constraints and strive to achieve its mission under budget pressures, the FTC conducts its work with resources that may be too limited. With a larger budget and proper oversight from Congress, the FTC's approach could be reoriented to pursuing cases with a high probability of success in federal court. This contrasts with the FTC's occasional practice of pursuing deception or unfairness cases that may not meet the statutory thresholds for success on the merits and entering settlements. For example, the FTC has, on occasion, issued complaints that include allegations of "unfair acts or practices," without analyzing whether the benefits of those acts or practices are outweighed by the harms they present, which consumers cannot otherwise avoid.

Federal statute requires this analysis, and yet the FTC has simply ignored it in some cases, perhaps in part because courts have not weighed in much on the kinds of evidence and considerations the FTC must introduce to meet the test.

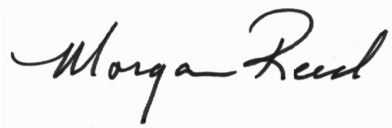
In light of recent data misuse reports, including allegations involving Cambridge Analytica, the FTC should be working to define the meaning of "unfairness" in the courts to accompany the excellent work it has been doing to conduct privacy workshops and craft guidance materials. Pursuing companies it suspects of violating Section 5 of the FTC Act with a consent order in mind as the end goal may be an optimal approach in some cases; but ultimately, consumers, small businesses, and the economy as a whole would benefit from the establishment of enforceable legal privacy norms through the pursuit of actual cases in federal court. To the extent more resources, oversight from Congress, and shifting of internal processes at the FTC are necessary to achieve this improved approach, the App Association would support those concepts.

Simultaneously, Congress should be working to clarify prohibited commercial privacy activity outside of deception ("unfair acts or practices" under current law); and establish enforceable statutory provisions that appropriately balance consumer protection from data misuse with the ability to flexibly use data to innovate for consumers' benefit (including to create better privacy tools). We support such federal legislation if it establishes a single, national standard. In the meantime, however, we encourage the FTC to seek legal clarity on privacy by pursuing strong Section 5 cases in court.

III. Conclusion

Congressional action to establish a federal privacy regime will undoubtedly require a difficult political process. Experience suggests that members of Congress are not likely to share the exact same views on all aspects of the privacy debate, whether on or off the committees of jurisdiction, regardless of party. Compounding the complexity of the issue, a general framework that avoids upending regulations covering industries with expert regulators and existing privacy regimes—like financial services and healthcare—would nonetheless cover a wide variety of different industries with unique enough business models that a single framework is unlikely to perfectly fit any of them. For these reasons, NTIA's leadership in publishing a set of goals and desired outcomes, informed by expert commentary, empirical evidence, and industry input, is of utmost importance. We look forward to working with NTIA, Congress, the FTC, the National Institute for Standards and Technology, and other stakeholders on crafting a national framework that protects privacy, prosperity, and American economic leadership.

Sincerely,



President
ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130