August 20, 2018

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex C)
Washington, District of Columbia 20580

Comments of ACT | The App Association to the Federal Trade Commission on Competition and Consumer Protection in the 21st Century (Question 5: "The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters")

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to provide input on the Federal Trade Commission's (FTC or Commission) upcoming hearings on whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy,[1] specifically regarding "the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters."

The App Association represents thousands of small business software application development companies and technology firms that create the software apps used on mobile devices and in enterprise systems around the globe. Today, the ecosystem the App Association represents – which we call the app economy – is valued at approximately $950 billion and is responsible for 4.7 million American jobs. Alongside the world's rapid embrace of mobile technology, our members have been creating innovative solutions that power the internet of things (IoT) across modalities and segments of the economy. The FTC's approach to competition and consumer protection enforcement law, enforcement priorities, and policy directly impacts each of the App Association's members.

[1] Federal Trade Commission, *Hearings on Competition and Consumer Protection in the 21st Century*, Notice of Hearings and Request for Comments, 83 FR 38307 (August 6. 2018).

II. The efficacy of the Commission's use of its current authority

In general, the FTC has taken positive steps to translate its authority to enjoin unfair or deceptive acts or practices in or affecting commerce[2] in the context of data security and privacy matters. The App Association represents about 5,000 small to mid-sized mobile software and connected device companies across the nation and the globe. We were especially pleased with the efforts under Chairman Ramirez, Acting Chairman Maureen Ohlhausen, and current Chairman Joseph Simons to learn more about how small businesses understand their legal obligations to protect consumer data and produce guidance materials.[3]

Clear legal obligations have been difficult to discern given the breadth of the FTC's authority to enjoin unfair or deceptive acts or practices and the fast-moving development of the technologies at issue when there is a breach or misuse of consumer data. This difficulty is exacerbated for small businesses that often lack the resources to hire legal teams or law firms to develop comprehensive data security policies or deploy sophisticated privacy measures specific to their businesses. Occasionally, advocates point to the FTC's numerous consent orders currently in force in order to give other companies an idea of the kinds of conduct that are allowed and those practices the Commission may consider unlawful under Section 5 of the FTC Act. However, the "soft law" of consent orders is not binding on the Commission and certainly does not bind other entities besides those with which the FTC has entered into such an agreement. Thus, the App Association encourages the FTC to try cases in courts where possible, in order to test its own interpretation of its authorities in the data security and privacy contexts.

a. *Unfairness cases*

Congress attempted to constrain the FTC's discretion under this prong by clarifying in 1994 that an act or practice is only "unfair" if it is *likely* to cause *substantial* injury and if that injury is not outweighed by countervailing benefits.[4] Previous Commissions have implemented enforcement actions on unfair acts without first demonstrating that the acts caused, or were likely to cause, a substantial injury. We believe these actions also run afoul of the Commission's own policy regarding its analytical framework for enjoining an

[2] 15 U.S.C. Sec. 45(a)(2), empowering and directing the Commission to prevent certain entities from "using . . . unfair or deceptive practices in or affecting commerce."

[3] *See* Press Release, FTC to Launch Campaign to Help Small Businesses Strengthen Their Cyber Defenses, https://www.ftc.gov/news-events/press-releases/2018/04/ftc-launch-campaign-help-small-businesses-strengthen-their-cyber (last visited Aug. 13, 2018).

[4] H.R. 5510 114 Cong. (2016).

unfair act or practice.[5] The best examples of FTC complaints alleging unfairness counts are those that conduct the statutory balancing test. On the other hand, those that skip the step of weighing the "countervailing benefits" of the conduct at issue, or whether consumers themselves could avoid the harm, are inappropriate applications of the Commission's authority.

ASUSTeK[6] and *Ashley Madison*[7] are two complaints in which the Commission identified a likely substantial injury to consumers under Section 5(n) of the FTC Act. In those cases, the complaint either alleged that a substantial injury had occurred or that it was likely to occur. However, as is too often the case in FTC complaints, there is no analysis of any "countervailing benefits" of the conduct at issue. The Commission need not spend a great deal of time describing the countervailing benefits of taking shortcuts with data security. But in the App Association's view, to completely ignore this statutorily-required examination results in an incomplete analysis. In the dynamic market of mobile software and connected devices, companies should have an incentive to introduce new and innovative products on the market. If newer products that might produce enormous "countervailing benefits" also happen to produce small, unintended, and ill-defined harms, small innovators like App Association members may sustain mortal damage from an investigation or complaint issued by a federal agency like the FTC. The best legal advice would be to avoid introducing innovative products and services in the first place. Therefore, when drafting consumer protection complaints, it is especially important in the privacy and data security context—which is possibly the area of consumer protection law most relevant to the app economy—to conduct a serious balancing test each time the Commission alleges unfair conduct.

b. *Deception cases*

With respect to its deception allegations, we urge the Commission to be vigilant for two potential and observed pitfalls: 1) considering too broad a set of misstatements to be "material" to a consumer; and 2) conflating the analyses behind an unfairness count and a deception count. We disagree, for example, with the U.S. District Court in *FTC v. D-Link* that the Commission can "tie[] [an] unfairness claim to the representations underlying the deception claims."[8] Such a conflation would be a misapplication of the statutory authority to enjoin these distinct activities because unfairness requires a

[5] *See* Fed. Trade Comm'n, FTC Policy Statement on Unfairness, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (last visited Oct. 19, 2017) (writing "To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.").

[6] In the Matter of ASUSTeK Comp., Inc., Dkt. No. C-4587.

[7] *See Operators of AshleyMadision.com Settle FTC, State Charges Resulting From 2015 Data Brach that Exposed 36 Million Users' Profile Information*, FTC, https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting (Dec. 14, 2016).

[8] *Ftc v. D-Link*, Case No. 3:17-cv-00039-JD, at p. 9, *available at* https://assets.documentcloud.org/documents/4057498/D-Link-Motion-Ruling-9-19-17.pdf.

separate statutory analysis.[9] Moreover, with California's requirement to publish a privacy policy--coupled with the fact that smaller businesses like our member companies have few spare resources to draft the perfect privacy policy--small, irrelevant misstatements are bound to appear. A dynamic business with fast-changing software products to adapt to consumer needs and demands is unlikely to be able to keep every aspect of its privacy policy entirely accurate with a high level of precision. This is why the Commission wisely declines to issue a complaint for a misstatement buried deep in a privacy policy that is unlikely to materially impact a consumer's decison making with respect to the product or service at issue.

III. The identification of additional tools or authorities the Commission may need to adequately deter unfair and deceptive conduct related to privacy and data security

In our experience, competition drives the use of robust cybersecurity risk management practices more than any other factor. The exploitation of a single security flaw can destroy customer confidence, and our member companies tirelessly work to implement robust and scalable data security measures, such as secure coding and other security-by-design principles. We are at the center of efforts to drive better security and privacy through public-private partnerships. For example, we support the National Institute of Standards and Technology (NIST) voluntary cybersecurity framework and have filed comments on the latest draft. We also support the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) system.

c. Any data security or privacy mandate should be based on risk and scalable to small businesses

A requirement to secure data or maintain the privacy of consumer data should be flexible along two key dimensions. First, any requirement should respect the ongoing and evolving privacy dialogue that exists between companies and the consumers they serve, so that the notice and choice they are presented with works best with the type of service or product and other contextual factors. Second, consistent with the Commission's own enforcement principles, any mandates beyond the current FTC Act should be scalable to the size, scope, and complexity of a business's operations. Small businesses like App Association members are simply not on the same compliance level as larger tech-driven firms that have teams of hundreds of compliance staff.

[9] 15 U.S.C. § 45(n).

d. Policymakers should pursue a single, national standard

With approximately 12 separate state-level data security regimes, varying requirements apply to our member companies depending on where the subjects of the data live. For example, Massachusetts requires our member companies to maintain a written, "comprehensive information security program," including "[r]eviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information."[10] These types of prescriptive regulations put our member companies under threat of penalty if they fail to review comprehensive data security plans when the Massachusetts Attorney General's office believes its business practices have undergone a significant enough change.

e. Regulatory authority and enforcement should be constrained, but more resources are needed for the FTC

We believe that if Congress grants new authorities for the FTC in data security or privacy, it should clarify that the Commission has the primary responsibility to enforce that authority, without upending privacy regimes covering protected health information, financial institutions, or education privacy regulations. Moreover, data security requirements should not empower officials with political incentives to subjectively interpret detailed requirements. Further, states should not be allowed to push small companies across the nation toward a minimum set of data security practices that fail to keep pace with the ingenuity of cyber attackers. Instead, data security requirements should incent innovative methods of data security and allow for flexibility depending on a company's size, the complexity of its operation, the sensitivity of the data and its uses, and the cost of security tools and measures. Moreover, in order to police the diverse types of businesses that fall under the FTC's jurisdiction, Congress should ensure that the Commission is reauthorized and has adequate resources to bring enforcement actions.

f. Policymakers should consider a presumption of compliance

One way of ensuring that a requirement is flexible and risk-based is to create a presumption of compliance for companies that take certain risk-based security measures. These measures should incent small companies to regularly monitor, assess, and upgrade their data security practices and technical measures. Creating such a framework would afford much-needed predictability for companies at a time when the contours of reasonableness are increasingly confusing.

[10] http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

g. No criminal penalties or private right of action

Companies have substantial market incentives to secure their systems and protect valuable data, as breaches of confidential personal information have repeatedly resulted in substantial economic loss to the companies and the displacement of senior management. Most data breaches are also the result of criminal acts. Therefore, federal legislation should not create criminal sanctions or penalties for these entities that are victims of a crime. An effective breach notification requirement and an efficient enforcement framework provide the best protection for consumers and will avoid unnecessary and frivolous litigation.

IV. Conclusion

The FTC is an able enforcement agency with a long history of fairly preventing the adverse consequences that arise from the evolving uses of data, while preserving their ability to produce novel benefits for consumers. The Commission's use of its current authority has placed it among the best privacy and data security enforcers in the world. But the Commission could make much-needed improvements through more rigorous analysis of unfairness cases and adherence to its own guidance in deception cases. New authority for the Commission could benefit the economy and strengthen consumer privacy if it is done carefully and if it establishes a single, national standard. We look forward to working with the Commission as it conducts this inquiry and continues to refine its approach to privacy and data security.

Sincerely,

Graham Dufault
Senior Director for Public Policy

Brian Scarpelli
Senior Global Policy Counsel

Joel Thayer
Policy Counsel

Madeline Zick
Public Policy Coordinator

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