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 4: "The intersection between privacy, big data, and competition")

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit views to the Federal Trade Commission (FTC) to inform its 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 intersection between privacy, big data, and competition."

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).

In its request for comment, the FTC seeks input on "the intersection between privacy, big data, and competition." Our members are at the forefront of discovery as far as big data's uses and are committed to the protection of consumer data and avoiding informational harms. For small businesses whose customers have strong data security and privacy expectations, utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. Consumers depend on our members to keep their valuable data safe and secure, therefore, maintaining consumer trust is the bedrock for our members' success, and they respect the efforts and enforcement authority of various competition agencies. Our members are committed to advancing consumer protection priorities by upholding the agency's enforcement actions, consent orders, and policy guidance.

The dynamic and hyper-competitive app ecosystem demands the use of robust risk management practices to keep consumers and their data secure. Our members know that the exploitation of a single security flaw can easily hamper customer confidence at an existential level. Lax data security or unenforced privacy practices can hurt companies with even the best reputations, which is why the App Association and its members tirelessly work to implement robust data security measures, implement secure coding, and utilize security-by-design principles. In fact, the App Association co-chaired the development of the United States Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council IV (CSRIC) Working Group 6, which developed security-by-design recommendations, best practices, and voluntary assurance mechanisms for securing core communications networks.[2]

Regardless of the conclusions drawn from the FTC's hearings, the App Association implores the FTC to uphold the following to establish competitive harm in the context of big data: (1) a clear definition of the relevant market; (2) a clear demonstration of market power; and (3) abuse of that market power. The potential for the internet of things (IoT)—an all-encompassing concept that includes everyday products that use the internet to communicate data collected through sensors—is vast, and we have yet to see the exciting new innovations and efficiencies it will bring. Our members utilize IoT to enable improved efficiencies in processes, products, and services across every sector, and this industry sector is projected to be worth more than $14.5 trillion by 2022.[3] With IoT at its nascent stage, we urge the FTC to base future actions on informational injuries on concrete consumer harms, rather than theoretical complaints alleging unfair acts or practices. Similarly, in complaints that allege deceptive acts or practices, the FTC should appropriately analyze the materiality of the case at issue. The future of IoT depends on common sense enforcement from administrative agencies around the world, and we implore the FTC to continue to demonstrate global leadership.

---

[2] See https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability#block-menu-block-4.

[3] "Global IoT Market Value Could Exceed $14 Trillion," ECN (April 2018), *available at* https://www.ecnmag.com/blog/2018/04/infographic-global-iot-market-value-could-exceed-14-trillion.

II. What is Big Data?

The real power of IoT comes from the actionable information gathered by sensors embedded in connected devices. IoT devices collect and share data, the most valuable of which becomes part of the commonly known "big data." The depth and potential of the term "big data" are amorphous. The App Association defines the term to mean structured or unstructured data sets so large or complex that traditional data processing applications cannot sufficiently analyze them. As sensors become smaller, cheaper, more accurate, and easier to use in connected devices, their big data analytics will secure more efficiencies across consumer and enterprise use cases.

Our members use IoT in a variety of ways, and broader IoT deployment will depend on specific use cases. For example, data and artificial intelligence (AI) will drive the future of medicine. A successful physician might see about 15,000 patients throughout their career, but our members create data-driven platforms that enable doctors to make decisions based on hundreds of thousands, even millions, of patient examples. With these software tools, a doctor can plug in a patient's characteristics and find the most effective medication or treatment. However, these benefits cannot be realized if companies are too afraid of incurring ill-defined liabilities for using AI under federal statutes.

Another example is the use of IoT for self-driving cars. Human error causes the clear majority of traffic accidents; however, the proper use of technology can help save lives. While the introduction of airbags, safety belts, and other innovations helped reduce traffic fatalities, the use of big data to analyze the causes and outcomes of traffic accidents can help us understand and address future accidents to exponentially reduce risk to countless Americans on the road. Self-driving cars will run on data from drivers and traffic patterns from around the globe. The machine-learning engine that cars use gathers driving data from vehicles in all their forms and in millions of different contexts, helping to distinguish a pedestrian from a bike from a tree. Technologists and regulators cannot predict the future life-saving uses for this data, nor can they identify the unintended harms that may result, but the data will have meaningful contributions to our society.

These are just two examples of how the dynamic app ecosystem and big data have introduced unexpected efficiencies across all sectors of our economy. While IoT sensors can be found in devices across sectors and industries, apps remain the main interface for communicating with these devices. We have yet to realize the full potential of an AI and machine learning-enabled IoT ecosystem. Therefore, we must ensure the app ecosystem continues to thrive and grow and that government agencies exercise regulatory humility so that these innovations can flourish.

III. Distinguishing Amongst Types of Big Data

The types of data can be broken into three main buckets: (1) volunteered data (i.e., user-shared data); (2) observed data (e.g., analytics from the volunteered data); and (3) inferred data (analytics from both volunteered and observed data).[4] These distinctions serve as a good marker as to when a company actually owns the data versus as opposed to when they merely have access to the data, making them important for competition. As the FTC is aware, access does not imply ownership, because data sets are not unique to any one company. For example, a consumer may utilize a Microsoft Surface to access a Gmail account; or a consumer who owns an Apple iPad could use it to access a Microsoft Outlook account. These scenarios demonstrate that one consumer can utilize at least two types of platforms, which can access the same information from the same consumer for different reasons. While all the companies have access to the data, none of them control access to that data. Regulators must overcome the challenge to examine what entity has access to what data before concluding the existence of a competition issue.

Another key issue regulators face is understanding the economic value of unique data sets created by AI or machine learning. Useless data today could transform into valuable data a year later based on its use and context. Unwarranted and/or premature interjection of competition law enforcement into this burgeoning economy can also negatively influence these beneficial outcomes.

The App Association believes that the big data economy is poised to accelerate the AI and machine-learning revolution, and it is premature to draw conclusions about the challenges we will face. Further, the App Association cautions the FTC to base any action it takes with respect to privacy, big data, and competition on data-driven, demonstrated harms, not hypotheticals.

[4] Greg Sivinski, Alex Okuliar, & Lars Kjolbye, *Is Big Data a Big Deal? A Competition Law Approach to Big Data*, European Competition Journal (2017), *available at* https://doi.org/10.1080/17441056.2017.1362866.

IV. Specific Recommendations on the FTC's Approach to Privacy, Big Data, and Competition

Based on the above, we offer the following recommendations regarding unfair acts or practices; and deceptive acts for consideration by the FTC in its forthcoming hearings.

a. Unfair Acts or Practices

Section 5(n) of the FTC Act provides the FTC with a balancing test to check its enforcement authority over unfair business practices. Unfortunately, previous FTC commissioners have interpreted "likely" to merely mean "possible" when addressing consumer harms, allowing the FTC to include commercial activity that could result in under-demonstrated and/or theoretical harms. The App Association believes that the FTC should not deem an act or practice unfair unless it is injurious in its net effects, and we support efforts to hold the FTC to this innovation- and consumer-friendly approach. Further, we strongly encourage the FTC to avoid ensnaring small companies in costly government proceedings to fight ill-defined allegations of "unfair" acts or practices.

b. Deceptive Acts

The App Association appreciates that the FTC may enjoin deceptive acts or practices in, or affecting, commerce;[5] in these cases, the FTC does not need to show likely concrete harm, as long as the deception has a material impact on consumers. In general, the FTC has handled this authority in a balanced manner that allows innovative products and services to reach consumers without misleading them materially. However, we believe the FTC must work to clarify how it determines the "materiality" of deceptive statements.

While the FTC does not need to demonstrate injury in deception cases, it must prove: (1) the company made a representation, omission, or practice that is likely to mislead the consumer; (2) the consumer's interpretation of that representation, omission, or practice is reasonable; and (3) the misleading representation, omission, or practice is material.[6] In some ways, the materiality element is controversial because the FTC's interpretation of the concept has become increasingly vague. The FTC's Deception Policy Statement indicates that certain types of claims create a rebuttable presumption of materiality.[7] However, the Commission should always consider the "competent and relevant evidence offered" when analyzing this element of deception. If the FTC refuses to consider the materiality element, then it will unduly complicate privacy procedures in the IoT context, particularly negatively impacting small business innovators. The

[5] 15 U.S.C. § 45(a).

[6] Fed. Trade. Comm'n, FTC Policy Statement on Deception, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (last visited Aug 19, 2018) (Deception Policy Statement).

[7] *Id.*

resulting reduction in investment and innovation would slow the evolution of the app economy and deprive the consumers who benefit from its growth.

Relatedly, we reject the holding in *FTC v. D-Link* that the FTC can "tie [an] unfairness claim to the representations underlying the deception claims."[8] This fusion of analyses would muddle the distinct frameworks the FTC uses to define an "unfair" or a "deceptive" act. In the App Association's view, the two analytical frameworks are distinct and must remain separate.

However, the App Association supports the FTC's efforts to explore types of informational injury and operationalize the types of evidence needed to erasonably quantify such injuries. However, we ultimately believe that such an inquiry should start with the statute that authorizes the agency to penalize the acts or practices that lead to informational injuries. The FTC has previously expanded its interpretation of statutory authority to include any act or practice that "causes or is likely to cause substantial injury to consumers"[9] in the context of privacy and data security. In some instances, the FTC has initiated actions against an entity even though it could not find a substantial injury to consumers, nor could it establish that an injury was likely to occur as a result of the alleged act or practice.[10] Without a rigorous analysis framework, the FTC will be operating outside of its statutory guardrails, inevitably pursuing hypothetical injuries in a manner that will hinder small businesses' investment and innovation.

[8] *FTC v. D-Link*, Case No. 3:17-cv-00039-JD, at p. 9.

[9] 15 U.S.C. § 45(n).

[10] *E.g.*, *In the Matter of Nomi Technologies, Inc.*, Dkt. No. C-4538.

V. Conclusion

The App Association appreciates the FTC's consideration of our responses to this question and urges FTC to contact the undersigned with any questions or ways that we can assist the FTC moving forward.

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