November 17, 2017

Competition Promotion Branch
Competition Bureau
50 Victoria Street
Gatineau, Quebec
K1A 0C9

Dear Sir or Madam:

ACT | The App Association (App Association) appreciates the opportunity to comment on the Competition Bureau's (Bureau's) white paper on big data and innovation.[1] This white paper attempts to tackle an important and complicated issue. The members we represent rely on consistent competition laws, therefore we proffer these suggestions for the Bureau's review and consideration as it continues its ongoing research on the Bureau's role in the big data-driven economy. A key concern we have with the paper is that it does not provide a concrete definition of what constitutes a relevant market in the "big data" context, making an antitrust analysis difficult and speculative. Moreover, the artificial intelligence (AI) and machine-learning revolution is in its infancy; any conclusion drawn at this stage is premature.

The App Association represents more than 5,000 small and medium-sized software application (app) companies and information technology firms throughout the $143 billion app ecosystem.[2] Our members leverage the connectivity of smartphones and mobile devices to create innovative solutions that make our lives better. The App Association advocates for an environment that inspires and rewards innovation while providing resources to help our members utilize their intellectual assets to raise capital, create jobs, and promote growth.

[1] Competition Bureau, Big Data and Innovation: Implications for Competition Policy in Canada, White Paper (2017), found here: http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04304.html.

[2] Brian Scarpelli, Nick Miller, & Roya Stephens, State of the App Economy, ACT | THE APP ASSOCATION (5th ed., Apr. 21, 2017), at https://actonline.org/wp-content/uploads/App_Economy_Report_2017_Digital.pdf.

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

Our members are committed to the protection of consumer data and avoiding informational harms if the data is compromised. 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 to protect consumers. 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 and scalable data security measures and institute secure coding and other 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.[3]

Regardless of the conclusions drawn from the Bureau's investigation in this proceeding, the App Association implores the Bureau to observe and uphold the ubiquitously accepted triumvirate to establish competitive harm: 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 $947 billion by 2019.[4] With IoT at its nascent stage, we urge the Bureau 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 Commission should appropriately analyze the materiality of the case at

---

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

[4] "Internet of Things Market and M2M Communication by Technologies, Platforms and Services (RFID, Sensor Nodes, Gateways, Cloud Management, NFC, ZigBee, SCADA, Software Platform, System Integrators), by M2M Connections and by IoT Components - Global Forecasts to 2019," MarketsandMarkets (November 2014), available at http://www.marketsandmarkets.com/Purchase/purchase_report1.asp?id=573.

issue. The future of IoT depends on common sense enforcement from administrative agencies like Canada's Competition Bureau.

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, however, for this paper, we loosely define 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 AI will drive the future of medicine. A successful physician might see about 15,000 patients throughout her 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. In 2015, Canada experienced an increase in traffic fatalities, and logged more than 10,280 serious injuries;[5] the majority of these types of accidents are caused by human error. However, the proper use of technology can help save lives. The introduction of airbags, safety belts, and other innovations helped reduce traffic fatalities in the United States from a high of nearly 55,000 in 1972, and the use of big data to analyze the causes and outcomes of traffic accidents can help us understand and address future accidents. 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 identity the unintended harms that may result, but the data will have meaningful contributions to our society.

[5] https://www.tc.gc.ca/eng/motorvehiclesafety/tp-tp3322-2015-1487.html.

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.

Distinguishing Types of Data

With the growth and potential of the IoT, regulators are faced with questions about who has access to what data. The types of data can be broken into three main buckets: 1) data that is volunteered (i.e., user-shared data); 2) data that is observed (e.g., analytics from the volunteered data); and 3) inferred data (analytics from both volunteered and observed data).[6] These distinctions are important for competition analysis because they 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. As the Bureau 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. We reiterate that we are in the infancy of the AI and machine-learning revolution and it is premature to draw conclusions about the challenges we will face.

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

Defining the So-Called "Big Data" Market

The first step in exercising antitrust analysis is defining the relevant market, and we appreciate the Bureau's observation of the nuances in its definition of the term "big data." From the perspective of competition law, not all data is equal. This creates difficulties when defining a market, and makes traditional analysis by Canadian agencies (e.g., the "hypothetical monopolists test") obsolete or insufficient. However, Canada is not alone in its struggle to define such an obtuse enterprise, and the United States is also struggling to define big data's relevant market.

In the United States, monopoly enforcement under Section 2 of the Sherman Act requires a party to demonstrate that the defendant has dominant market power in the relevant market.[7] However, certain lower courts, particularly in the Ninth Circuit, have been cavalier in their interpretation of what constitutes a "relevant market," sparking concern from legal experts seeking to reconcile courts' determinations in the matter.[8] Most believe the definition of a relevant market "is the most critical tool in antitrust enforcement..."[9] but unfortunately, Congress did not provide courts with a test to determine an industry's relevant market.[10] In order to make this determination, courts will look to the elasticity of demand in the entire market, and the cross-elasticity of supply of substitutes.[11] In essence, a court must assess the availability of a substitute product for the customer—and whether the customer would favor the substitute product if there were a slight increase in the price of the main product—to determine the relevant market.[12] However, there is a lot of ambiguity in a product's elasticity, which may invite undisciplined interpretations that could defeat its purpose.

---

[7] *U.S. v. Grinnell Corp.*, 384 U.S. 563, 570-71 (1966).

[8] E.g., Robert Pitofsky, *New Definitions of Relevant Market and the Assault on Antitrust*, 90 Colum. L. Rev. 1805, 1806-07 (1990).

[9] E.g., Pitofsky at 1806-07.

[10] See *Brown Shoe v. U.S.*, 370 U.S. 294, 321 (1962).

[11] *United States v. E.I. du Pont de Nemours & Co.*, 351 U.S. 377 (1956) [hereinafter Cellophane].

[12] *Grinnell*, at 571-72.

Moreover, the issue of relevant market assessment is further complicated by the Department of Justice's (DOJ's) Merger Guidelines (Guidelines). Scholars have long lamented the Guidelines and their effectiveness.[13] Before the Guidelines, three leading cases served as the triumvirate for courts engaging in relevant market analysis. See id. at 1813. Those cases are: 1) *Cellophane*; 2) *Brown Shoe Co. v. U.S.*;[14] and 3) *Grinnell.*[15] These cases represent the myriad ways in which courts define a relevant market, and are incidentally cumbersome when applied to the internet economy.

Though the internet has provided remarkable economic growth and interconnectivity to the global community, it continues to befuddle judges and legal scholars in the antitrust context.[16] In fact, many courts are reticent to even attempt to define the relevant market in an internet context for fear of limiting the internet's expansive reach.[17] This inability to define the relevant market becomes even more problematic because the two premier antitrust agencies—the DOJ and the FTC—use these decisions to inform their enforcement actions.

Separately, while the challenges articulated in the Bureau's white paper are apt, they are incomplete because they assume a market without establishing one. Specifically, characterizations in the paper do not make clear who is competing with whom and fail to define the commodity being sold. For instance, the white paper does not make a meaningful distinction between companies that collect data versus those that have access to data. As such, it is hard to determine whether the Bureau would consider an agriculture equipment company, like Massey Ferguson, a competitor of Google if it collects data on annual crop yields from its machines and provides it to its customers. Or is the third-party developer that provides the middleware to Massey Ferguson that enables its machines to use the data considered Google's competitor? These determinations are important

---

[13] Pitofsky at 1808 ("[m]any of the problems that have plagued definition of relevant market in the antitrust field can be traced to the inherent difficulty of measuring market power, and to the inadequate analysis used in three important Supreme Court decisions. Various problems have emerged as a result of the inconsistent approaches taken in these cases.").

[14] 370 U.S. 294 (1964).

[15] *See* Pitofsky, at 1813-16.

[16] *E.g.*, Jared Kagan, *Bricks, Mortar, and Google: Defining The Relevant Antitrust Market For Internet-Based Companies*, 55 NYL Sch. L. Rev. 271, 278 (2010) (writing "While newly emerging Internet companies may very well raise antitrust concerns, it is not certain how the relevant antitrust markets in which these companies operate will be defined. This is due to the fact that courts have not yet had much experience defining these markets. David S. Evans, the scholar who has predicted many of these antitrust issues, even recognizes that defining the relevant market for these Internet firms involves some uncertainty.").

[17] *E.g.*, *American Online, Inc. v. GreatDeals.Net*, 49 F.Supp.2d 851 (E.D. VA 1999) (holding "With respect to the relevant geographic market in which competition takes place, the Court finds that the Internet cannot be defined with outer boundaries. It is not a place or location; it is infinite. Internet is a "giant network which interconnects innumerable smaller groups of linked computer networks." The network "allows any of literally tens of millions of people with access to the Internet to exchange information.").

because without a clear relevant market, any subsequent analysis on market power is dubious.

We encourage the Bureau to clarify how it intends to categorize the relevant market in the context of big data and identify the appropriate market participants. Regardless of the requisite market share needed to show market power, it must still define the relevant market.[18] Moreover, the Bureau should make clear whether it is discussing data as an actual product or as an input. Any competition agency's essential question should be whether the data is the asset, or ancillary to the business model, where the data is input to feed their economic objective. If the answer is the latter, and data is ancillary to the business model, this definition encompasses a myriad of industries and is not quantifiable for antitrust analysis.

Determining Market Power

We agree with the Bureau that the determination of market power is a key factor when determining an abuse of power, and depends on finding market power and merger analysis. Under the Bureau's own rulings, the mere presence of a company with a large market share is not enough to raise concerns under Canada's Competition Act (Act),[19] but the Bureau must first demonstrate that a company possesses enough market share to exert market power.

We appreciate the Bureau's consideration of the European Commission's (EC's) decision in the Microsoft-LinkedIn merger when discussing its view on the challenges in assessing market power. We agree with the Bureau's analysis that the EC considered the relevant factors when determining that the merger did not create competition concerns because LinkedIn has other competitors with access to the same databases and information.

In the United States, courts interpret Section 2 of the Sherman Act as requiring parties to prove two conditions to establish the existence of a monopoly: (1) "the possession of monopoly power in the relevant market;" and (2) "the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident."[20] Moreover, the courts define a monopoly as having "the power to control prices or exclude competition."[21] The existence of such power may ordinarily be inferred from the predominant share of the market.[22] In American Tobacco v. U.S., the U.S. Supreme Court held that "over two-thirds of the entire

[18] *Grinnell*, at 571.

[19] Competition Bureau, Position Statement, Competition Bureau Statement Regarding Its Investigation into Alleged Anti-Competitive Conduct by Google, 19 April 2016.

[20] *Grinnell Corp.* at570-71 (1966).

[21] *See id.*

[22] *See id* at 571.

domestic field of cigarettes, and "over 80% of the field of comparable cigarettes' constituted 'a substantial monopoly."[23] In U.S. v. Aluminum Co. of America, the Second Circuit held that a company must obtain 90 percent of the relevant market share to be considered a monopoly.[24] However, the United States Supreme Court provided a threshold to determine dominant market share when it wrote, "it is doubtful whether sixty or sixty-four percent [of a particular market] would be enough, and certainly thirty-three percent is not."[25]

With these considerations in mind, the App Association believes the following framework is helpful in addressing the issue of finding "market power" and conducting merger analysis in the context of big data. The Bureau must:

1. Find what data is relevant to the market competitors;
2. Determine whether the data is commercially available as a "product" or as an "input" for downstream competitors;
3. Determine whether the market participant owns the data or only has access to the data; and
4. Determine whether the data is unique to the market participant.[26]

Given the nascent nature of the AI and machine-learning economy, the Bureau should incorporate this nimble framework when defining the relevant market for this growing field.

A Clear Demonstration of an Abuse of Market Power

As we previously outlined, the mere presence of a company with a large market share is not enough to raise concerns under the Competition Act.[27] Antitrust law is not designed to punish companies for being successful but is instead meant to protect and benefit consumers.[28] However, there are threshold issues at play in this proceeding, particularly the lack of a concrete definition of the relevant market for big data, and the Bureau should first address these issues before requesting comment on policy prescriptions. We strongly urge the Bureau to always demonstrate a clear abuse of market power before deciding to take action.

[23] 328 U.S. 781, 797 (1946).

[24] 148 F.2d 416, 429 (2d Cir. 1945).

[25] *See id.*

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

[27] Competition Bureau, Position Statement, Competition Bureau Statement Regarding Its Investigation into Alleged Anti-Competitive Conduct by Google, 19 April 2016.

[28] Marvin Ammori, *Monopolies: Antitrust Law Protects Consumers, Not Competitors*, Wired (16 Oct. 2012, 3:00 PM).

The App Association Suggests This Framework for Informational Injuries to Promote IoT-Enabled Economy and Protect the Rights of Canadian Consumers

The App Association cautions the Bureau from acting on competition claims concerning informational injuries before it demonstrates a concrete harm. We provide the following guidance for the Bureau's consideration:

A. For Unfair Acts or Practices

The Bureau has requested comment on which regulatory frameworks would be helpful to ensure the agency can strike a balance between protecting consumers' privacy and maintaining financially feasible requirements on platforms to protect the data. The App Association encourages the Bureau to look to the U.S. Federal Trade Commission's (FTC) regulatory framework when developing enforcement procedures for platforms that violate their privacy policies.

In the United States, 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 theoretical harms. We agree with FTC Acting Chairman Ohlhausen that the Commission should not deem an act or practice unfair unless it is injurious in its net effects, and we support her efforts to hold the Commission to this innovation- and consumer-friendly approach.

We strongly encourage the Bureau to avoid ensnaring small companies in costly government proceedings to fight ill-defined allegations of "unfair" acts or practices. These proceedings often force companies to undertake the unenviable task of proving a negative—they must prove that their products will never be accessed by unauthorized third parties. These burdensome and onerous regulatory measures jeopardize both the success of small business app developers and the ever-growing IoT ecosystem.

B. Deceptive Acts

For deceptive acts, the App Association recommends that the Bureau encourage a legal framework that mirrors that of the U.S. FTC. Under its organic statute, the FTC may enjoin deceptive acts or practices in, or affecting, commerce.[29] 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. While we encourage the Bureau to consider the FTC's framework, we believe

[29] 15 U.S.C. § 45(a).

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.[30]

In many 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.[31] However, the Commission should always consider the "competent and relevant evidence offered" when analyzing this element of deception. If the Commission refuses to consider the materiality element, then it will unduly complicate privacy procedures in the IoT context. The Commission sees consent decrees as de facto rulemaking authority. However, if the FTC's framework, and any other like it, continues to implement these decrees without examining materiality, app and other IoT companies will become increasingly reticent to expand their businesses or engage with traditional brick-and-mortar institutions to better serve their customers.[32] If the Commission does not execute a proper deception analysis that includes an evaluation of materiality, then small business app companies will not want to incur the significant liability faced when fighting an FTC proceeding, particularly for actions they do not control. The outcome would produce net negatives for the app economy, the evolution of the IoT ecosystem, and the consumers who benefit from both.

Relatedly, we reject the U.S. District Court's notion in *FTC v. D-Link* that the Commission can "tie[] [an] unfairness claim to the representations underlying the deception claims."[33] This fusion of analyses would muddle the distinct frameworks the Commission uses to define an "unfair" or a "deceptive" act. The two analytical frameworks are distinct and must remain separate. When considering the FTC's framework, the Bureau should provide an

---

[30] Fed. Trade. Comm'n, FTC Policy Statement on Deception, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (last visited Oct. 19, 2017) (Deception Policy Statement).

[31] *See id.*

[32] Geoffrey Manne, R. Ben Sperry, & Berin Szoka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case*, INTERNATIONAL CENTER FOR LAW & ECONOMICS, http://docs.techfreedom.org/ICLE_TF_Nomi_Comments_5.27.15.pdf (2015).

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

updated concept of "materiality" that does not adopt the district court's prescription to combine the analyses.

We strongly support, and encourage the Bureau to consider, the FTC's efforts to explore types of "informational injury" and operationalize the types of evidence needed to prove their existence. However, we ultimately believe the 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"[34] in the context of privacy and data security. In some instances, the FTC 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.[35] Without a strong analysis framework, the FTC operated outside of its statutory guardrails, freeing it to pursue hypothetical injuries in a manner that hurt small businesses and innovators.[36] We urge the Bureau to consider the benefits, nuance, and challenges of the FTC framework when developing a Canadian framework for informational injuries to promote the IoT enabled economy.

[34] 15 U.S.C. § 45(n).

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

[36] *E.g.*, *In the matter of LabMD*, Dkt. No. 9357; see also, Dune Lawrence, A Leak Wounded This Company. Fighting the Feds Finished It Off, BLOOMBERG, https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/ (Apr. 25, 2016).

Conclusion

The App Association hopes the Bureau considers the suggestions and explanations we have provided while developing its forthcoming framework.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Associate Policy Counsel

Brad Simonich
Associate

ACT | The App Association
1401 K St NW (Suite 501)
Washington, District of Columbia 20005