

October 27, 2017

Federal Trade Commission, Office of the Secretary
Constitution Center, 400 7th Ave, SW, 5th Floor, Suite 5610 (Annex A)
Washington, District of Columbia 20024

RE: *Comments of ACT | The App Association for Informational Injury Workshop
P175413*

ACT | The App Association (App Association) appreciates the opportunity to provide input on the Federal Trade Commission's (FTC or Commission) upcoming Informational Injury Workshop.¹

I. Introduction

The App Association represents more than 5,000 small and medium sized software application (app) companies and informational technology firms across the \$143 billion app ecosystem.² Our members leverage the connectivity of smart phones and 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. We believe that the planned FTC Informational Injury Workshop represents an important step in the right direction to establish sustainable frameworks. On behalf of our members, we hope these frameworks accomplish two overarching goals: 1) help small businesses better understand the types of activities that can lead to data security and privacy enforcement actions; and 2) ensure the Commission conducts rigorous analyses so that allegations of unfair or deceptive practices meet statutory constraints.

¹ Fed. Trade Comm'n, Public Notice on Information Injury Workshop, <https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop> (last visited Oct. 9, 2017).

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

Our members maintain a strong commitment to the protection of consumer data and avoiding informational harms when that consumer data is compromised. Using the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity for small businesses whose customers have strong data security and privacy expectations. Earning and maintaining consumer trust is the bedrock for our members' success – they each respect the FTC's efforts to protect consumers, as well as the FTC's ultimate enforcement authority. The App Association's members are committed to advancing FTC consumer protection priorities through its enforcement actions, consent orders, and policy guidance.

The dynamic and hyper-competitive app ecosystem demands the use of robust risk management practices. Our members know that the exploitation of a single security flaw can easily hamper customer confidence at an existential level. Lax data security or unfair privacy practices can hurt companies with even the best reputation, which is why the App Association and its members tirelessly work to implement robust and scalable data security measures and implement secure coding and other security-by-design principles. In fact, the App Association co-chaired the development of the FCC's Communications Security, Reliability, and Interoperability Council IV (CSRIC) Working Group 6, which developed security-by-design recommendations and best practices and voluntary assurance mechanisms for securing core communications networks.³

We urge the Commission to base its future actions on informational injuries on concrete consumer harms, rather than theoretical complaints alleging unfair acts or practices. Similarly, in the complaints that allege deceptive acts or practices, the Commission should appropriately analyze the materiality of the case at issue. The future of the internet of things (IoT) depends on common-sense enforcement from administrative agencies like the FTC.

IoT is an all-encompassing concept that includes everyday products that use the internet to communicate data collected through sensors. Our members utilize IoT to enable improved efficiencies in processes, products, and services across every sector, and it is projected to be worth more than \$947 billion by 2019.⁴

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.

The real power of IoT comes from the actionable information gathered by sensors embedded in every connected device. IoT devices collect and share data, the most valuable of which becomes part of the commonly known “big data.” We define this term to mean structured or unstructured data sets so large or complex that traditional data processing applications are not sufficient for analysis. 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 we know that broader IoT deployment will be very use case-dependent. For example, data and artificial intelligence (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. Every year, the United States has more than 35,000 traffic fatalities, the majority of which are caused by human error. However, the proper use of technology can help save lives. Airbags, safety belts, and other innovations helped reduce traffic fatalities from a high of nearly 55,000 in 1972, but the use of large volumes of 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. While technologists and regulators cannot predict the future life-saving uses for this data or the unintended harms that may result, we do ourselves a disservice if we ignore their potential benefits due to unknown, theoretical injuries.

These are just two examples of how the dynamic app ecosystem has introduced unexpected efficiencies across all sectors of our economy, in less than a decade of existence. While IoT sensors can be found in devices across sectors and industries, mobile apps on smartphones remain the main interface for communicating with these devices. Therefore, the continued success of the IoT revolution depends on the app economy’s continued innovation and growth. It also depends on government agencies exercising regulatory humility to ensure these innovations can flourish.

We strongly support the Commission's efforts to explore types of "informational injury" and operationalize the types of evidence needed to prove their existence. We recognize that the Commission's approach is forward-looking and proactive; however, the inquiry should start with the statute that authorizes the Commission to penalize the acts or practices that lead to informational injuries. In previous administrations, the Commission expanded its interpretation of statutory authority to include any act or practice that "causes or is likely to cause substantial injury to consumers"⁵ in the context of privacy and data security. In some instances, the Commission 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.⁶ 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.⁷

Given the cost associated with FTC proceedings, small business app developers like our members do not have the time or capital to fight claims based on hypothetical harms to consumers. Sadly, these investigations have put small companies out of business due to the resources required to respond to investigative demands. The ability to source and obtain capital for their businesses is extremely important for small business app developers, and our members would attest that time taken away from these endeavors could jeopardize their businesses altogether.⁸

⁵ 15 U.S.C. § 45(n).

⁶ *E.g.*, *In the Matter of Nomi Technologies, Inc.*, Dkt. No. C-4538.

⁷ *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).

⁸ Joel Thayer, *To Innovate, We Must Repatriate*, ACT | The App Association (Apr. 18, 2017) (writing "[f]or small businesses, access to capital is crucial, and members of ACT | THE APP ASSOCIATION understand this all too well. Small businesses in the app economy participate in an integrated and collaborative market, in which they rely on the technologies, platforms, and investments of much larger firms to operate.") <http://actonline.org/2017/04/18/to-innovate-we-must-repatriate/>.

We applaud the Commission for aligning itself with the spirit of Section 5 of the FTC Act, which promises to implement enforcement actions against likely concrete harms (as opposed to speculative harms) for alleged unfair acts or practices that affect commerce. We are encouraged by the Commission's efforts to define categories of informational harms, particularly in privacy and data security cases. The informational injuries proposed by Chairwoman Ohlhausen—from health and safety to unwarranted intrusion—are practical and workable. It is a welcomed departure from previous FTC filings where the Commission failed to describe the types of harms that have occurred or could occur.⁹ Additionally, the Chairman's proposed framework appropriately moves away from the occasions in which the Commission exceeded its legal authority by basing its enforcement actions on theorized harms and not on an established likelihood of substantial injury.¹⁰ We believe it is vital that the Commission outline the categories of informational harms and update the analytical frameworks to help the Commission clearly articulate likely informational injuries in data security or privacy cases.

II. Suggested Framework for Informational Injuries Under Section 5 of the FTC Act

A. Unfair Acts or Practices

A prong of the Commission's "consumer protection" jurisdiction, the authority to include *unfair* acts or practices has created a lot of controversy. 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.¹¹ 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 unfair act or practice.¹²

⁹ See *Infra*. § III.

¹⁰ See *id.*

¹¹ H.R. 5510 114 Cong. (2016).

¹² 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.").

Section 5(n) provides the Commission with a balancing test to check its enforcement authority over unfair business practices. However, previous FTC commissioners interpreted “likely” to merely mean “possible,” allowing the FTC to include commercial activity that could result in theoretical harms. The defendants’ reluctance to challenge these determinations in court, and the FTC’s ability to stray from its statutory constraints, threatens innovations whose effects are not fully understood, including the evolving IoT ecosystem. As a result, we agree with Chairwoman Ohlhausen that the Commission should not deem an act or practice unfair unless it is injurious in its net effects. We also support her efforts to hold the Commission to this innovation- and consumer-friendly approach.

We strongly encourage the Commission to avoid ensnaring small companies in costly federal proceedings to fight ill-defined allegations of “unfair” acts or practices. These proceedings often force them to undertake the unenviable task of proving a negative—that their products will never be accessed by unauthorized third parties. These burdensome, onerous, and often unwanted consent decrees jeopardize both the success of small business app developers and the ever-growing IoT ecosystem.

B. Deceptive Acts

Under its organic statute, the FTC may enjoin *deceptive* acts or practices in, or affecting, commerce.¹³ In these cases, the FTC does not need to show likely concrete harm, as long as the deception at issue is material to consumers. In general, the FTC has handled this prong of its 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.

As previously stated, the FTC does not need to demonstrate injury in deception cases, but it must show:

- 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*.¹⁴

¹³ 15 U.S.C. § 45(a).

¹⁴ 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).

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.¹⁵ 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 continues to implement these decrees without examining materiality, app and other IoT companies will become increasingly reticent expand their businesses or engage with traditional brick-and-mortar institutions to better serve their customers.¹⁶ For instance, if the Commission does not execute a proper deception analysis that includes an evaluation of materiality, then small business app companies are unlikely to want to incur the extraordinary liability involved in fighting an FTC proceeding for actions they don’t control. This yields net negatives 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.”¹⁷ Such a fusion of analyses would further muddle the distinct frameworks the Commission uses for an “unfair” or a “deceptive” act. The two analytical frameworks are distinct and must remain separate. Moving forward, the FTC should update the concept of “materiality,” but we urge them to not adopt the district court’s prescription to combine the analyses.

¹⁵ See *id.*

¹⁶ 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).

¹⁷ *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>.

III. Prior FTC Complaints Using a Proper Consumer Injury Analysis Should Inform the Commission's Informational Injury Framework Going Forward

We offer the following examples of FTC actions against entities where it established a concrete harm and materiality to better assist the Commission in making future determinations:

a. Unfair Acts or Practices

*Ashley Madison*¹⁸

Ashley Madison, a website catered to users in search of extra-marital relationships, had its networks breached by intruders *several* times between November 2014 and June 2015.¹⁹ Due to the website's security flaws, a pastor tragically committed suicide after hackers publicly placed his name on the list of people using the website.²⁰ Due to the unfortunate outcomes of the data disclosure and the amount of times the website was actually accessed by unauthorized third parties, the Commission acted appropriately and should categorize its injuries as those affecting health or safety.

*ASUSTeK*²¹

The FTC found that Taiwan-based computer hardware maker ASUSTeK Computer, Inc., had critical security flaws in its routers that put the home networks of hundreds of thousands of consumers at risk. Their administrative complaint also charged that the insecure design of its "personal cloud" offering led to the unlawful disclosure of data on thousands of consumers' connected storage devices, which led to the exposure of their sensitive personal information on the internet. Based on its investigation, the FTC found that unauthorized third parties accessed roughly 12,900 consumers' connected USB storage devices in 2014.²² Within this case, the Commission established the link between unauthorized access by third parties and harm to the victims, a critical element missing from other edge cases alleging informational injuries. We encourage the Commission to categorize this type of injury as an unwarranted intrusion that is likely to result in financial injury.

¹⁸ See *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach 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).

¹⁹ See *id.*

²⁰ Laurie Segall, *Pastor Outed on Ashley Madison Commits Suicide*, CNNMONEY (Sept. 8, 2015), <http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html>.

²¹ *In the Matter of ASUSTeK Comp., Inc.*, Dkt. No. C-4587.

²² *ASUS*, at p. 8.

Ultimately, the boundaries of an informational injury from an unwarranted intrusion are especially difficult to define. Evidence for other types of informational harms more directly support the existence of those harms, therefore we believe the Commission should find a way to operationalize its analysis for this category of informational injury. Otherwise, it could become a catch-all to implicate acts or practices unlikely to result in substantial harm. In these cases, we encourage the Commission to consider several factors, including: 1) whether unauthorized access occurred; 2) if so, the breadth of the unauthorized access (i.e., how many consumers' data, networks, devices, etc., were breached); 3) the sensitivity of the data, network, device, etc., at issue; 4) the nature of the entity responsible for the unauthorized access; 5) the behavior of the entity or entities responsible for the unauthorized access; and 6) the level of exposure of the data, network, device, etc. (i.e., what does the unauthorized access allow hackers to do with the data, network, device, etc.). Adding up these factors could help decipher whether substantial injury has occurred or is likely to occur, in the form of an unwarranted intrusion, even when the likelihood of financial, health, safety, or other more specific harms cannot be established.

b. Deceptive Acts or Practices

*Practice Fusion*²³

The FTC charged Practice Fusion with soliciting and posting reviews from patients online, without taking any steps to conceal personally identifiable information. According to the FTC's complaint, Practice Fusion sent emails to patients of healthcare providers that used its electronic health records service and requested they participate in an online survey. Practice Fusion intended the patients' responses to the survey to be entered into their public-facing healthcare provider directory. However, Practice Fusion failed to disclose this intent to participating patients, many of whom were under the impression that their survey responses would remain private. The survey yielded extremely sensitive personal information from the patients (e.g., patients' medication prescriptions), which was displayed publicly on Practice Fusion's public website. The Commission found that these victims were not likely to have shared this sensitive information if Practice Fusion made the survey's intention known to them. Thus, the FTC appropriately found that the practice at issue subverted consumer choice by hiding a clearly material aspect of Practice Fusion's handling of sensitive data.

²³ *In the Matter of Practice Fusion*, Dkt. No. C-4591.

IV. The Commission Should Avoid Analytical Mistakes Made in Some Prior FTC Cases as it Crafts Analytical Frameworks for Informational Injuries

The following cases are ones where the FTC found no concrete harms to satisfy substantial injury under Section 5(n) or failed to show “materiality” under Section 5(a):

A. Unfair Acts or Practices

LabMD

In this case, the FTC failed to show any actual, or likely, consumer harm. The FTC claimed that LabMD did not adequately protect its consumer data because it was easily accessible to other peer-to-peer networks. However, there was no evidence that the consumer data had been compromised, accessed, taken, or used by an unauthorized third party. In fact, the Commission’s own Administrative Law Judge (ALJ) rejected its claim, stating that, “at best [the Commission] has proven the ‘possibility’ of harm, but not any ‘probability’ or likelihood of harm.”²⁴ The FTC’s extensive discovery process to determine whether consumer data was compromised resulted in an expensive investigative demand process, as well as an administrative case that inadvertently put LabMD out of business.²⁵ This case underscores the important need to analyze the nature of the allegedly unauthorized access, as well as the type of entity that allegedly perpetrated the breach. As a rule, we believe the Commission should avoid issuing complaints where the only entity that has potentially unauthorized possession of data is a research firm with no reason to use it in a manner that harms consumers. We urge the Commission to clarify that informational injury is unlikely to occur when there is no evidence to suggest that the entity with unauthorized possession of consumer data intends to use it to harm consumers.

²⁴ *LabMD*, at 48.

²⁵ 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).

*D-Link*²⁶

The evidence gathered in this case clearly suggests that D-Link's security practices were lacking—the use of hard-coded login credentials as the sole data security method is widely known to put connected devices at risk. However, we agree with the U.S. District Court of California's holding that the Commission must find that an actual harm occurred or that D-Link's actions were likely to lead to an injury.²⁷ Though D-Link failed to use adequate security measures, the Commission could not demonstrate a likelihood of substantial injury to consumers because it did not present any evidence that consumer data had been accessed or used.²⁸ The mere existence of a security flaw should not be representative of a likelihood of harm when the Commission alleges an unfair act or practice. This broad interpretation of the statute would enable the Commission to halt innovative products and services based on the expectation of hypothetical consumer injuries. This kind of preemptive enforcement is especially threatening to the dynamic, small-business driven app economy.

The FTC should clarify that in data security cases of alleged unfair acts or practices, substantial injury is generally unlikely if there is no evidence to suggest that unauthorized access occurred. Without this basic finding, the Commission is unable to describe the type of informational harm that is likely to occur. Guessing the type of injury that might result from D-Link's security failures is not based on evidence and would be an undisciplined expansion of the FTC's statutory authority. In cases where informational harm is likely to result from an act or practice, the Commission must articulate a category of informational injury with a finding based on evidence.

²⁶ See *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras*, FTC Press Release, <https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate> (Jan. 5, 2017).

²⁷ *FTC v. D-Link*, Case No. 3:17-cv-00039-JD, found here: <https://assets.documentcloud.org/documents/4057498/D-Link-Motion-Ruling-9-19-17.pdf>.

²⁸ See *id.* at p. 8.

*HTC*²⁹

HTC added Carrier IQ, a third-party app, to its handsets that use the Android operating system. HTC preinstalled Carrier IQ without giving the smartphone user the option to remove the application, nor did they notify the user that the app was even installed. According to the FTC complaint, HTC used an insecure method to shuttle data to the Carrier IQ software, however, the FTC declined to articulate the likelihood of any specific informational injury. The Commission speculated that a hacker could send “text messages without permission,”³⁰ but they did not provide any evidence to support a theory of likely harm, nor did it detail the type of informational injury that was likely to result. The Commission must take these steps in future unfairness cases, and should clarify its actions in future public materials. These steps are especially important for companies like our members, who plan on using machine-learning capabilities in their products. With their software tools, it is unclear how data will be used in any particular context, so preemptively preventing acts or practices that are not likely to cause articulable harm is a real threat to their usefulness and success. Cases like *HTC* send a negative signal to companies. If they can think of any negative outcome of an AI-driven app, they may be liable under the FTC Act, ultimately preventing them from bringing their product to market, or worse, encouraging them to opt out of the IoT market altogether.

B. Deceptive Acts or Practices

*Nomi*³¹

In this proceeding, the Commission did not consider the totality of circumstances when assessing the materiality of the alleged deceptive claims. Nomi—a data analytics company—received permission from participating brick-and-mortar stores to place sensors in retail stores to collect data on certain consumer behavior via the consumers’ cell phones. Nomi issued a privacy statement claiming that consumers could opt-out of this data collection at “any of its clients’ retail stores” when, in reality, consumers could only opt-out on Nomi’s website. Within this case, the first two elements of deception were met—Nomi misrepresented the opt-out provision and consumers reasonably believed they could opt-out of Nomi’s services at participating retail stores. However, the Commission failed to demonstrate the materiality of Nomi’s privacy statement. Under the Commission’s own guidelines, it must consider the “competent and relevant evidence offered” to evaluate whether consumers would have chosen not to engage with a product or service but for the statement at issue. The Commission *did not* use this analytical framework in the Nomi case, and we therefore encourage the Commission to first ensure that it follows its existing analytical frameworks as it considers new frameworks for informational harm.

²⁹ *In the Matter of HTC America Inc.*, Dkt. No. C-4406.

³⁰ HTC Complaint, *In the Matter of HTC America Inc.*, Dkt. No. C-4406, available at <https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222htccmpt.pdf>.

³¹ *In the Matter of Nomi Technologies, Inc.*, Dkt. No. C-4538.

V. Conclusion

The App Association appreciates this opportunity to comment on the Commission's efforts to define informational injuries to better support the innovations and efficiencies created by app developers and tech firms across the country. We hope that the perspectives we shared will help the Commission develop appropriate analytical frameworks, based on the classifications of informational injuries and within the statutory rights of the Commission. We have learned lessons from prior FTC cases, and we firmly believe that the FTC framework and the assessment of potential injury to consumers' data privacy and security is based on evidentiary support. Our small tech companies and app innovators often take calculated risks to create innovative, industry-shaking products that benefit consumers – their ability to do so is jeopardized if they do not have clear guidelines that define their liability under federal law.

Respectfully submitted,

/S/

Brian Scarpelli
Senior Policy Counsel

/S/

Graham Dufault
Director of Government Affairs

/S/

Joel Thayer
Associate Policy Counsel

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