The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
Washington, District of Columbia 20515

April 10, 2018

Dear Chairman Walden and Ranking Member Pallone:

ACT | The App Association appreciates the opportunity to comment on this important hearing to examine how companies use consumer data and communicate with consumers about those uses. This hearing, "Facebook: Transparency and Use of Consumer Data," affords us the opportunity to examine how the small companies that plug into larger platforms like Facebook handle these major issues. The sobering revelations around Cambridge Analytica have underscored that now more than ever, quietly seeking extraordinary data privacy permissions is not a viable approach. In this letter, we will share what we have learned through our efforts to educate on privacy law compliance and the development of best practices and describe the benefits of allowing some flexibility for consumers and companies to define permissible uses of data from the perspective of small tech businesses.

The app ecosystem is now valued at roughly $143 billion and represents the front end for $8 trillion in international trade annually. The impressive numbers produced by this powerful engine are driven by small enterprises. Most of our members range from one-person shops to a few hundred people at the most. Yet some of the most significant advances in data-driven industries, from healthcare and public safety to manufacturing and smart cities, come from small businesses like App Association member companies. This gives us a unique voice on data privacy issues.

The United States leads the world in digital innovation. Why? Because American companies are at the forefront of using data to produce beneficial services. With over seven million tech sector jobs, and a growth rate of 3 percent, the policy environment in the United States has produced a successful, data-driven economy, and countries all over the world are working to expand their tech sectors as well. We must take steps to ensure continued growth for the United States, while addressing the serious privacy problems this hearing sets out to explore.

With this statement, we hope members of the Committee take away the following:

- Our experience suggests that effective privacy protection requires a persistent dialogue between data collectors and consumers tailored to the circumstances of and purposes for data collection and use;

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

- Industry groups like ACT | The App Association are working hard to ensure small and mid-sized firms understand how to comply with legal obligations, while leveraging competition in the market to create new approaches to protect privacy; and

- Overly intrusive government regulation of privacy—including strict data minimization or constant opt-in requirements—is suboptimal because it would interrupt the privacy dialogue that should be occurring between companies and consumers and may strip away uses of large data sets that are unforeseeable at the time of collection.

I. Industry Efforts to Enhance Consumer Privacy

Consumer privacy is a difficult concept to standardize because it can mean so many different things to different people. Further complicating the differing values and definitions of ideal privacy are the increasingly important and complex uses of data that pertain to individuals. The events that led to this hearing—a situation where consumer data was shared in a manner that appears consistent with an agreement's terms, but further uses by a third party were not authorized—illustrate these difficulties well. Nonetheless, the App Association has participated in and led several industry efforts to enhance consumers' options, develop best practices, and hold companies accountable for their actions related to consumer privacy. Some lessons learned in these processes may help the Committee as it considers possible market failure and its own role in better protecting consumer privacy.

Most relevant to this hearing, the App Association a) executed the practical application of the National Telecommunications and Information Administration (NTIA) multistakeholder group's short form privacy notice; and b) led the creation of several compliance guides and best practices, including conducting privacy events called the mobile developer ("MoDev") series, the Health Insurance Portability and Accountability Act (HIPAA), and the European Commission's General Data Protection Directive (GDPR).

A. NTIA short form privacy notice

In 2013, NTIA hosted a multistakeholder working group gathering consumer groups together with industry 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.[1]

The final product called for signatories to the code of conduct to disclose any information they collect in eight key areas including biometrics and financial information, as well as whether they share with certain types of entities including ad networks and carriers. Stakeholders from the American Civil Liberties Union (ACLU) to Verizon supported the final code of conduct and on July 25, 2013, the group moved on to the testing phase. The App Association developed user interfaces and reported on consumer testing of some physical representations of the short form notice code of conduct. Some observations may be relevant as the Committee examines the issues raised by Cambridge Analytica's alleged retention and use of consumer data.

[1] https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

First, in an effort to shorten privacy notices, the resulting privacy dashboard describing the basics of how and with whom an app shares data would leave out the "why." During testing, consumers indicated that they were confused as to why a given app would collect certain information. For example, one consumer wondered why a fitness tracking app would collect financial information (perhaps the app would collect financial information only if the consumer purchased something through the app). Another wondered why an app shared any information with a social network and what that social network would do with the information. When consumers are asked to examine privacy policies closely and think about what app companies are doing with their data, questions quickly arise, and short form notice does not lend itself easily to an explanation of "why" certain data is collected or shared with certain entities.

Second, consumers were confused by notices using icons without interactive features. In the image above, types of data the app does not collect are signified with a faded icon and the word "NO." But consumers looking to learn more about the app company's decision-making with respect to their data were frustrated when tapping the icons did not pull up further details. This result suggests that a short and simple privacy notice should also include an option to learn more, as well as an option to turn on or off the app's collection of a certain type of information, as some mobile platforms allow us to do now.

Third, participants in the testing did not understand the role of certain types of entities indicated in the short form notice. The types of companies they understood the least included "consumer data resellers" and "data analytics providers." Thus, even when an app developer makes it clear that it shares specific types of data with data analytics providers, consumers lacked an understanding of what data analytics providers or consumer data resellers *do* with their information and the repercussions that could ensue.

The findings from our short form notice testing show that to be truly useful and accessible, privacy must be an interactive dialogue between the service and the consumer. As software has improved, we have better capabilities to facilitate this interaction and many of those improved functionalities have manifested themselves in the market. Even as small to mid-sized app developers like our member companies create innovative privacy dialogues with their users, the privacy options available on some platforms play an important role. The technical controls available for consumers—whether provided through the app or at the platform level—obviate

the need for platforms to conduct audits on apps to find out whether they are complying with a contractual term. That control is already vested in the consumer.

We have found that privacy controls on the iOS platform are highly effective and maintain the ability for app developers and consumers to share valuable information, which helps ensure their services remain free and the next great product is based on actionable data. Platform privacy options have the powerful attribute of not allowing app developers to circumvent them, which in turn gives app developers confidence that consumer wishes are being honored through the platform. However, the Committee should avoid governmental mandates that require such controls. Just as compliance with the bare minimum aspects of a voluntary program results in suboptimal privacy protections, so would a mandate remove the incentives for companies to compete and experiment with other solutions. Similarly, a mandate requiring a platform to conduct audits on all the apps that plug into it would have the perverse effect of pushing competitively sensitive information to the platform that could be used to advantage it against smaller potential competitors. Moreover, these mandates would incent companies to undertake those baseline measures to comply with the letter of the law, leading to stagnant privacy models that fail to grow with better technologies and evolving consumer needs.

B. Compliance Guides and Best Practices

Platforms can provide valuable privacy-enhancing functions for app developers and consumers. But App Association members do not rely completely on platforms to comply with global privacy laws on their behalf. The Cambridge Analytica situation underscores that platforms and the companies that use platforms to reach consumers are separate entities, and neither one can be completely responsible for the other. Small businesses like App Association members may not have the considerable resources of platform companies to hire compliance staff or attorneys, but they are often just as liable under privacy laws here and abroad. The App Association acts as a resource for small businesses by producing compliance guides that make legal privacy obligations understandable and accessible for small, growing companies.

In our GDPR compliance guide, we note that when app companies share data with a third-party data processor, they must always seek written assurance from the data processor of "sufficient guarantees" that it also complies with GDPR.[2] We counsel our member companies to play the game of "Mother, May I," with a controller's data (in many cases the platform company). The definitions and interrelationships contemplated in GDPR are complex, and explaining them in short form is extremely difficult. But the guide is an example of private sector efforts to ensure that even the smallest companies in the app ecosystem are observing the most stringent privacy laws on the books. We are making serious efforts to ensure that small and mid-sized firms in the app economy are not taking advantage of their distance from the consumer.

We note that GDPR is not necessary to keep companies honest in this regard and would not have stopped activities in which Cambridge Analytica is alleged to have engaged. If good actors like our member companies do not have the direct consumer relationship, they do not benefit from taking advantage of the opacity of their activities involving consumer data. Not only do those activities risk running afoul of U.S. privacy law, but they also undermine the trust on which those companies' brands are built. We have found that compliance with GDPR is extremely expensive and diverts resources away from needed areas of growth, and even privacy policy development. One App Association member company with just under 60 employees has dedicated 10 full-time staff to developing its own compliance program with GDPR. And once the

[2] http://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf

program is completed, two full-time staff are likely to be tasked with continued compliance with the law. We want to be clear that while we seek to clarify our member companies' legal obligations under European privacy law, we have seen firsthand that the law imposes unnecessarily high costs on small businesses.

The advent of app platforms democratized app development, creating a pathway for mobile software entrepreneurs to reach consumers in a safe and secure environment. As soon as this increased access for small business took place, the App Association began its privacy outreach to developers through its MoDev series. Thus, we sought to democratize privacy best practices in equal measure to the spread of business opportunity to small businesses. We conducted these seminars throughout the country and reached thousands of developers, delivering the message that app developers are responsible for clearly describing which data they collect, why they collect it, and what they do with it. Ten years ago, many developers were aware that they performed analytics, but had a less firm grasp on the fact that these analytics required the collection and stewardship of sensitive personal data. We conveyed the message that not only does this collection impose a serious responsibility on developers, but that responsibility also may be defined by policymakers in Washington if they failed to take appropriate measures to account for privacy.

App Association member companies that develop connected devices or apps that deal with health information ("protected health information" or PHI in healthcare parlance) face a potentially steep compliance burden under HIPAA. Our "HIPAA Check" tool guides app developers through a series of questions to determine how they can comply with the rules.[3] Although the tool is not legal advice, it helps give app developers a sense of the steps they need to take in order to put themselves on the right track. At the end of the process, we give the app company an option to receive a full, detailed report based on its answers to the questions.

With these guides and tools, the App Association and similar industry groups are "democratizing" an understanding of privacy obligations to smaller companies that plug into larger platforms. The alleged activities of Cambridge Analytica are an outlier among companies that draw consumer data from platforms. Although these kinds of events can evoke in the general public a sense that tech companies have come unmoored from privacy principles and accountability for the sake of monetizing the consumer's data, reality is less alarming and not nearly as sensational. Big data-driven products and services are not the "wild west" when it comes to seeking permission and adhering to promises around authorized uses of data. Legal privacy obligations are real, they apply to even the smallest businesses, and we are happy to make those obligations clear and accessible.

II. Beneficial Uses of Data are Incompatible with Strict "Minimization" or "Opt-In" Requirements

As the Committee considers its role in shaping future privacy obligations, we caution against inevitable calls to adopt a regulatory regime like Europe's, which could preclude some of the most innovative and life-saving corners of our economy. A mandate to delete information that has survived the purposes for which it was initially collected would clearly render Cambridge Analytica's alleged actions illegal, not just in violation of relevant contractual terms. But the mandate would also flush reams of data from the ecosystem that are being put to work to improve safety and create jobs.

[3] https://app.actonline.org/hipaa/disclaimer

Under GDPR, personal data may only be "collected for specified, explicit . . . purposes and not further processed in a manner that is incompatible with those purposes . . .."[4] The inherent nature of artificial intelligence makes this provision at least very difficult to comply with and in some cases impossible. The European rules also require companies to collect express "opt-in" consent before processing personal information, which must be "specific," "unambiguous," and made by "a statement or by a clear affirmative action."[5] There are a number of reasons policymakers should weigh the beneficial applications of artificial intelligence against policies that would wipe them out along with harmful actions like those at issue in this hearing.

A. Healthcare

Data-driven healthcare services provide an important example of why regulatory approaches should allow for flexible uses of data. Flexible data privacy laws support American jobs and can also save lives. The future of medicine is in data and artificial (or "augmented") intelligence, tools that enhance the diagnostic and treatment capabilities of healthcare providers. A successful physician might see about 15,000 patients throughout her career, but recent innovations in technology have grown providers' reach and effectiveness exponentially. Our members create data-driven platforms that enable doctors to make decisions based on hundreds of thousands, even millions, of examples. For instance, with these clinical decision support tools, a doctor can plug in a patient's characteristics and see which medication is most likely to work. But this functionality only works if the characteristics can be matched against countless data points that a strict data minimization mandate would require to have been deleted.

Cancer clusters provide another important example. Researchers have long puzzled over why certain types of cancer occur in certain regions at higher rates than other parts of the country. In order to truly examine the various sets of circumstances and factors that may play a role in these higher rates, sensitive data must be collected and processed in ways that are not initially foreseeable. A series of data points that may seem to have nothing to do with cancer could become the key to combating it, and requiring them to be deleted pulls the rug out from our cancer curing efforts.

These advantages benefit everyone, and yes, they can save lives. But they can only exist when personal data can be collected for purposes beyond those that can be articulated with specificity at the outset and stored despite having served their initial purposes. Moreover, a mandate that requires constantly seeking unambiguous, precise consent from consumers serves as an interruption of an ongoing privacy dialogue that should be taking place between a consumer and app developer. Our member companies know that policies requiring the deletion of personal information that does not have a perfectly defined purpose at the time it is collected seriously degrade these life-saving capabilities.

B. Self-Driving Vehicles

Machine learning, a subset of artificial intelligence, animates the other engines in self-driving cars—the autonomous driving application. Just as the physical engines run on energy, the

[4] https://gdpr-info.eu/art-5-gdpr/
[5] https://gdpr-info.eu/art-6-gdpr/; https://gdpr-info.eu/art-4-gdpr/

autonomous driving engine runs on data from drivers and traffic patterns from around the globe. How can a self-driving car recognize a the trajectory of another car or an animal crossing the road? How does it know the animal is not a tree or a bush? The machine-learning engine that cars use must have seen animals in all their forms, in millions of different contexts. American car companies must collect data that is inevitably personal in nature in order to inform the software that drives these cars. The data must be held and processed for an indefinite period of time and for a set of purposes that are not explicit, except insofar as they serve as a representation or example for the software to compare against countless other examples.

As self-driving cars evolve and their machine-learning engines improve, the data that serves as the basis for the machine-learning engine may be used in ways that are not foreseeable now and yet produce substantial safety benefits. Unlike livestock or pets that might cross a road, which to the software are "known unknowns," these are the "unknown unknowns"—potential threats that are not well enough understood to articulate them at the time images or other impressions of them are collected. If Congress were to enact policies requiring car companies to delete personal data (pictures of pedestrians for example) as soon as its future purposes are "incompatible" with the initial purpose, it would encumber their ability not just to create jobs, but also to save lives.

C. Business Intelligence

You may not realize that, on average, it takes your local coffee shop longer to make cold drinks than hot drinks. But the nation's coffee chains are acutely aware, and longer processes require more workers behind the counter. Coffee chains have discovered that warmer weather leads to more cold drink purchases, at different rates depending on which part of the country you are located. In one city, coffee consumers may switch at much higher rates to cold drinks for every five-degree rise in temperature than in another city. Other types of weather features likely play a role as well. Coffee chains use these trends to predict staffing levels as many days in advance as possible, to handle the longer time it takes to make cold drinks. All of this analysis requires the collection and processing of data indicating human behavior, which could include personal information. But coffee chains and other types of consumer-facing businesses do not only care about how weather affects consumer behavior—countless other factors play a role in necessary staffing levels and supply needs. We simply cannot predict which factors will tend to create which outcomes and strict data minimization and explicit opt-in consent models require this kind of prediction or else the data must not exist.

III. Conclusion

The revelations that brought about this Committee's examination of consumer data privacy are alarming examples of how data revealing patterns in human behavior can be used against consumer expectations. It is often said that consumer privacy is about context—but more than that, it is about time and location. We appreciate the opportunity to share the lessons we have learned from our experiences in providing compliance assistance but also in creating the user interface for best practices. We urge the Committee to take a cautious approach when considering policies that would negate the beneficial uses of data to try and obviate abuses. An approach that errs on the side of hamstringing data usage not only prevents the unforeseeable, yet beneficial, uses of that data, but it also subverts the approach to privacy that respects the ongoing and just-in-time dialogue companies that use data should be having with their customers.

Sincerely,

Morgan Reed
President
ACT | The App Association