ACT The App Association

April 21, 2017

Ms. Lisa Barton
Secretary of the Commission
United States International Trade Commission
500 E Street, S.W.
Washington, District of Columbia 20436

RE: USITC's Investigations into Digital Trade and the Impact of Barriers to Digital Trade on the Competitiveness of U.S. Firms in International Markets

Dear Ms. Barton:

In response to the opportunity for public comment issued on February 6, 2017[1], ACT | The App Association hereby submits comments to the United States International Trade Commission (USITC). Our written submission addresses USITC's public request for input on their investigations into uses of new digital technologies by U.S. companies and the impact of barriers to digital trade on the competitiveness of U.S. companies in international markets.

The App Association represents more than 5,000 small- and medium-sized software application development companies and high technology firms located across the United States.[2] As the world has quickly embraced mobile technology, our members have been creating innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives.

While the global digital economy holds great promise for small app development companies that must continue to grow to compete, our members face a diverse array of challenges entering new markets. These challenges are commonly referred to as "trade barriers," broadly defined as laws, regulations, policies, or practices that either protect domestic goods and services from foreign competition, artificially stimulate exports of domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights. These barriers take many forms but have the same net effect: impeding U.S. exports and investment.

[1] *Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions; Institution of Investigation and Scheduling of Hearing*, 82 Fed. Reg. 10397 (February 10, 2017).

[2] ACT | The App Association, *About*, *Available at* http://actonline.org/about.

We applaud USITC's efforts to understand and examine the most important foreign barriers affecting U.S. exports of goods and services, U.S. foreign direct investment, and protection of intellectual property rights. Further, we are committed to working with USITC and other stakeholders to reduce or eliminate these barriers. With respect to digital trade, the small business innovators we represent prioritize the following principles:

- ***Cross-Border Data Flows:*** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. Innovative small app development companies must be able to rely on these unfettered data flows as they seek access to new markets.
- ***Data Localization Policies:*** Companies looking to grow in new markets too often face regulations that force foreign providers to build and/or use local infrastructure in-country. These data localization requirements cause serious declines in imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our member companies do not have the resources to build or maintain unique infrastructure in every country in which they may do business, and such requirements effectively exclude them from commerce.
- ***Customs Duties on Digital Content:*** American app developers and technology companies need to take advantage of the internet's global nature to reach billions of new customers. However, the "tolling" of data crossing political borders to collect customs duties directly contributes to the balkanization and reduced efficiency of the internet and effectively blocks these innovative products and services from market entry.
- ***Requirements to Provide Source Code for Market Entry:*** Some governments have proposed putting into place policies requiring companies to give access to, or transfer, proprietary source code before being able to legally enter that country's marketplace. For app developers and tech companies, intellectual property is the lifeblood of their innovation, and transfer of source code to a government presents an untenable risk of theft and piracy. These requirements are serious disincentives to international trade and a non-starter for the App Association's members.

- ***The Ability to Use Strong Encryption Techniques to Protect End User Security and Privacy:*** Global digital trade depends on technical data protection methods such as the use of strong encryption techniques to keep users safe from harms such as identity theft. However, some interests persist in demanding that "back doors" be built into encryption for the purposes of government access, effectively. These policies would degrade the safety and security of data as well as the trust of end users by creating known vulnerabilities that unauthorized parties can exploit. The viability of a small app development company's product from a security and privacy standpoint depends on its end users' trust.
- ***Protection of Intellectual Property:*** The infringement and theft of intellectual property and trade secrets presents a major threat to the success of App Association members and, in turn, the billions of consumers who rely on these app-based digital products and services. These intellectual property violations can lead to customer data loss, interruption of service, revenue loss, and reputational damage – each of which is a potential "end-of-life" occurrence for a small app development company. Strong, but fair, protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential.

The App Association was pleased to testify on this matter during the April 4, 2017-held USTIC hearing, during which we also submitted written testimony available via the USITC's Electronic Document Information System. Based on our testimony and the above, the App Association highlights the following specific trade barriers faced by our members, and urges their incorporation into the USITC's findings. Though some of the issues noted below are proposals that may not yet be fully in force, we urge USITC to consider including them in its report.

CHINA

Issue: Proposed Internet Domain Name Management Rules

With more than 50 percent of its population online, China represents enormous potential for small business innovators to grow and and create new jobs while relying on the internet to reach new markets. The App Association's members face growing challenges to enter the Chinese market, including the internet regulatory regime in China. Attempts to filter or impede cross-border data flows continue to harm internet-related businesses and the consumers who use them.

We note that China's Ministry of Industry and Information Technology (MIIT) March 25, 2016-issued draft regulation titled "Internet Domain Name Management Rules (Opinion-seeking Revision Draft)"[3] which includes an article addressing China's power to not provide internet service to foreign internet sites, specifically states:

> Article 37: Domain names that connect to the network from within the borders shall have services provided by domestic domain name registration service bodies, and domestic domain name registration management bodies shall carry out operational management. For domain names that connect to the network from within the borders, but which are not managed by domestic domain name registration service bodies, internet access service providers may not provide network access services.

This article would allow any internet service provider in the country to block network access to a foreign website or internet-based business simply because their domain name is registered in a different country. The application of this regulation poses a significant threat that small business innovators from the App Association's membership may be selectively excluded from the Chinese marketplace to buoy domestic interests.

[3] Rogier Creemers*, Internet Domain Name Management Rules (Opinion-seeking Revision Draft*, China Copyright and Media (last updated Mar. 29, 2016), *Available at* https://chinacopyrightandmedia.wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/.

Issue: Proposed Regulation of "Pre-Installed Apps"

China's MIIT issued a proposed regulation regarding "pre-installed" apps on mobile handsets on April 7, 2016, which was also notified through the World Trade Organization's Technical Barriers to Trade (TBT) Committee.[4] Specifically, the regulation included proposals to:

- Permit end-users to remove pre-installed apps including those that are used for basic device functionality, effectively permitting software changes to operating system software when such a requirement would impede the ability of operating system operators to ubiquitously update devices' functionality and security, negatively impacting the integrity of both the manufacturer and internet service provider platforms, as well as the larger innovative app development ecosystem.
- Impose unnecessary or unrealistic app developer registration requirements that would add new barriers and costs to entering a platform's market, which would ultimately reduce the availability of apps for Chinese consumers.
- Mandate "specialized testing organizations" organized by the Chinese government that carry out supervision and inspection of pre-installed apps and that "related enterprises shall cooperate and provide convenient access to their application software," creating the possibility that app companies would have to give access to, or transfer, proprietary source code to Chinese authorities before being allowed to legally enter the Chinese marketplace.
- Have Chinese social organizations "establish blacklists of malicious application software" and share such lists among other stakeholders, without providing a process for social organizations which undertake app blacklisting exercises to give reasonable accessibility and process fairness principles.
- Require that mobile smart terminal application software "use digital certificates issued by lawfully established electronic authentication service agencies for signature" and that enterprises "use digital certificates for signed mobile smart terminal application software, to verify and mark clearly," without assuring that mobile smart terminal application software use digital certificates may be issued by any Certificate Authority that follows relevant international standards (as opposed to those mandated by the Chinese government).

[4] World Trade Organization, (G/TBT/N/CHN/1171), Technical Barriers to Trade Committee Notification, (Apr. 7, 2016). *Available at* http://www.spcr.cz/images/CHN1171.pdf.

The App Association submitted comments directly to MIIT, as well as through the TBT Committee, discussing our views on the above proposals[5] and how this proposed regulation's definitions and overly-prescriptive approach, if implemented, would risk restraining the highly-competitive and innovative mobile phone and app marketplace in China and will negatively affect the global digital economy.

Issue: Cyberspace Administration of China (CAC) Mobile App Regulation

In June of 2016, the CAC released, without seeking public input, a regulation addressing mobile app providers and mobile app stores, titled "Administrative Provisions on Information Services of Mobile Internet Application Programs."[6] This regulation contains numerous provisions intended to protect national security through requirements on app providers such as requiring the monitoring of online content and the reporting of violations to government authorities, as well as ensuring that new app users register with their real identities; and the monitoring of and taking action against users that publish "banned content" as well as the reporting of the same to Chinese government authorities. This regulation went into effect on August 1, 2016.

Issue: Various Data Localization Requirements (Proposed and Final)

Currently, China has either put into effect or has proposed numerous restrictions on the flow of data across its borders. These proposed or final regulations limit or prohibit the transfer of data from within China in such areas as banking and financial credit, cybersecurity, counter-terrorism, commercial information systems, healthcare, and insurance. Each represents a significant barrier to market entry and is, effectively, a non-starter for small business innovators who would otherwise look to the Chinese marketplace to expand their businesses and create jobs.

[5] ACT | The App Association, *RE: Interim Administration Regulation for Mobile Smart Terminal Application Software Pre-installation and Distribution*, (June 6, 2016). *Available at* https://actonline.org/wp-content/uploads/MIIT-Pre-Installated-App-Regulation-.pdf.

[6] Cyberspace Administration of China, *Provisions on the Management of Mobile Internet Applications' Information Services*, (June 28, 2016). *Available at* http://www.cac.gov.cn/2016-06/28/c_1119123114.htm.

Issue: Cybersecurity Law Taking Effect June 1, 2017

In November 2016, China's Standing Committee of the National People's Congress passed final legislation imposing new cybersecurity data governance requirements on companies doing business in China. The law applies to both "network operators," defined as anyone owning or operating a computer system network, and "suppliers of network products and services."[7] The new law addresses a comprehensive array of privacy and security regulations. The Chinese government has stated that this law is intended to protect national security by better safeguarding Chinese citizens' data and giving law enforcement more access to technological systems when needed.

The most concerning aspect of the law is the vagueness of its text, leaving the scope of the law precariously undefined. What is definitive in the law's language is that it applies to all foreign technology companies conducting business in China. The law requires foreign technology and data companies to build or maintain servers inside of China, so that the data of all Chinese citizens will be stored exclusively within China. This demand for data localization effectively means that technology companies, including many of the App Association's members, may be simply priced out of doing business in the Chinese market.

This law also mandates that companies provide "technical support" to Chinese law enforcement during an investigation, but it does not clearly define what that entails. In some cases, technical support to law enforcement could consist of a "backdoor" to the technical protection mechanisms on which software companies heavily rely to maintain customer trust, like encryption. If companies are required to create such a "backdoor" in the process of an investigation, they face the possibility of an eroded global customer base.

Issue: Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data

On April 11, 2017, the CAC released a draft titled "Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data" for public comment (due May 11).[8] While the App Association continues to evaluate this proposal and will be submitting views directly to the CAC, our preliminary assessment of the proposal has raised significant concern regarding the subjectivity of this proposal as well as its mandating of all "network operators" to self-assess the security of their cross-border data transfers and being subject to similar assessments by the Chinese government.

[7] http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

[8] www.cac.gov.cn/2017-04/11/c_1120785691.htm.

EUROPEAN UNION

Issue: Digital Single Market

The App Association supports the European Union's (EU) Digital Single Market (DSM) strategy's goals to open digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy. However, while the DSM benefits European businesses by facilitating business across the EU through e-commerce, it should also bring Europe into the global digital market. The App Association has advocated for the DSM to ensure that it does not set up barriers to the success of the DSM, such as requirements to store data locally or mandates to diminish the use of strong encryption.

We urge that the EU's DSM be included in the USITC's report to ensure that U.S. government remains engaged on this sweeping strategy from a trade barrier perspective. Already, as a part of the DSM, several consultations and proposals have been carried forward by the European Commission that raise significant concerns for the App Association, including:

- A DSM proposal to regulate online platforms;[9] and
- A DSM consultation on "safety risk" of apps widely,[10] when no safety risk exists solely due to using an app to access a good or service.

These include regulatory proposals for nascent economic segments and services that are solutions in search of a problem and should be pulled back. Activities under the DSM should be based on data-demonstrated public needs.

Issue: Proposed Rules on Encrypted Devices and Communications

European Justice Commissioner Věra Jourová announced on March 28th that the European Commission will release related rules on June 20th, 2017, that will grant law enforcement easier access to end-to-end encrypted data on electronic communications services like WhatsApp.[11] This follows public calls from officials in the United Kingdom, Germany, and France for law enforcement to have the same rights to access encrypted online services as they do to phone call information from telecommunication companies during criminal investigations.

[9] European Commission, *Online Platforms,* (last visited Oct. 25, 2016). *Available at* https://ec.europa.eu/digital-single-market/en/online-platforms-digital-single-

[10] Digital Europe, *Public consultation on the safety of apps and other non-embedded software not covered by sector-specific legislation*, (Sept. 15, 2016, 06:33PM). *Available at* http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2286&language=en-US&PortalId=0&TabId=353

[11] *See* Eurativ, "EU to propose new rules targeting encrypted apps in June," (Mar. 29, 2017), *available at* http://bit.ly/2phYX3C.

The approach proposed by Commissioner Jourová is seriously flawed from both a policy and a technical perspective. Any transaction involving data depends on technical data protection methods, such as the use of strong encryption techniques, to maintain user trust. Mandating the development of “backdoors” into encryption frameworks for the purposes of government access would not only degrade the safety and security of data, but also jeopardize the trust of end users by creating known vulnerabilities that unauthorized parties can exploit. Undermining the technical proficiency of encryption moves us away from, rather than towards, the legitimate policy goals that the App Association supports, including law enforcement’s proper and timely access to data.

INDONESIA

Issue: Data Localization Requirements on Electronic System Providers of Public Services

Indonesia's Ministry of Communications and Information Technology (MCIT) requires electronic system providers for public services to locate a data center and disaster recovery center within Indonesia.[12] While some larger companies may be able to absorb such a cost to provide their products and services to the Indonesian consumers and businesses, such requirements serve as a massive disincentive for the small tech innovators that the App Association represents, locking them out.

Issue: Proposed Regulations on 'Over The Top' Service Providers

The App Association has significant concern with the Ministry of Communication and Informatics' (Kominfo) *Draft Regulation of the Minister of Communications and Information of the Republic of Indonesia, Number ___ of 2016, concerning Provision of Application Services and/or Content over the Internet (OTT)*.[13] We believe that the proposal, if implemented, will create an overly burdensome regulatory environment in a number of ways that will hamper economic growth for Indonesia, including Indonesia's burgeoning mobile app developer business community. This proposed Kominfo regulation includes:

- Requiring a physical presence in Indonesia by OTT service providers when small businesses simply cannot afford to open local offices in every market in which they offer their services, nor can they afford to dedicate resources to establishing partnerships with local conglomerates. This requirement would create a cost burden to market entry that is untenable for small businesses, particularly in the case of attaining licensing from the Investment Coordination Board.
- Mandatory partnerships between OTT service providers and telecommunication providers, when such a policy would be extremely expensive for all OTT service providers (as defined by Kominfo), and particularly onerous for small app makers.

[12] *See* Mary R. Silaban, *Unleashing Indonesia's Digital Innovation*, American Chamber of Commerce in Indonesia (June 10, 2014). *Available at* http://www.amcham.or.id/fe/4614-unleashing-indonesia-s-digital-innovation. *See also*, U.S. Dep't of State Bureau of Economic and Business Affairs, *2014 Investment Climate Statement – Indonesia*, (June, 2014). *Available at* http://www.state.gov/documents/organization/226821.pdf.

[13] Republic of Indonesia's Ministry of Communication and Information Technology, *Draft Number 3 of 2016 concerning Provision of Over-The-Top Application and/or Content Services via the Internet,* (Mar. 31, 2016). *Available at* http://www.lexology.com/library/detail.aspx?g=4aa11c3e-cf65-4998-921a-2ac8408b375b.

- Requiring the localization of data storage or processing, specifically (1) the use of national payment gateways that are legally incorporated in Indonesia, specifically for paid OTT services; (2) the use of an Indonesian internet protocol number and placing part of the server in data centers in Indonesia; and (3) the local storage of data for a minimum of three (3) months, or longer should law enforcement request it.

On May 26, 2016, the App Association filed detailed comments with Kominfo describing the difficulties posed by many of the specific provisions in the draft OTT regulation, which we urge the Trade Policy Staff Committee to review.[14] Further, we respectfully requested that Kominfo refrain from implementing this regulation and engage in further consultation with affected stakeholders to allow for meaningful and win-win solutions to concerns that Kominfo may have in seeking to regulate OTT services. While this regulation remains in draft form, we request that it be included in USITC's investigation into barriers to digital trade.

[14] ACT | The App Association, *RE: Kominfo's Draft Regulation, Number ___ of 2016, Provision of Application Services and/or Content over the Internet (OTT),* (May 26, 2016). *Available at* http://actonline.org/wp-content/uploads/act_comments_to_kominfo_re_draft_ott_regulation_052616-1.pdf.

INDIA

Issue: Various Proposed and Final Restrictive Data Localization Laws

India has in place and is considering policies that restrict the flow of data across its borders and create significant issues for small business innovators seeking to expand into the Indian market, including:

- India's National Data Sharing and Accessibility Policy requires that all data collected using public funds to be stored within the borders of India.[15]
- The 2015 National Telecom M2M ("machine to machine") Roadmap,[16] which has not been implemented, states that all M2M gateways and application servers serving customers in India need to be located within India. The draft policy also proposes that foreign SIM cards should not be permitted in devices to be used in India.

Issue: Continuing Threats and Uncertainty Regarding the Ability to Use Strong Encryption

Currently, Indian internet providers must attain government approval from the Telecom Regulation Authority of India (TRAI) to employ encryption stronger than 40-bit encryption. Further, as recently as late 2015, the Indian government proposed a National Encryption Policy that presented numerous proposals of significant concern to the App Association. As this is an ongoing issue of serious concern to small business innovators, we recommend that it be included in the investigation to ensure continued prioritization for the U.S. government and other stakeholders.

[15] Government of India Ministry of Science & Technology, *India's National Data Sharing and Accessibility Policy*, (2012). *Available at* http://ogpl.gov.in/NDSAP/NDSAP-30Jan2012.pdf.

[16] Government of India Ministry of Communications & Information Technology Department of Telecommunications, *National Telecom M2M Roadmap*. *Available at* http://www.gsma.com/connectedliving/wp-content/uploads/2015/05/150513-DoT-National-Telecom-M2M-Roadmap.pdf.

NIGERIA

Issue: Comprehensive ICT Localization Rule

The Nigerian government issued its "Guidelines for Nigerian Content Development in Information and Communications Technology,"[17] which raise a myriad of concerns for our members. The Nigerian government imposes extreme localization requirements on multinational companies. For instance, section 10.3 of the Nigerian government's guidelines mandates multinational companies to not only store their data in Nigeria but also requires such companies to incorporate 50 percent of local products when manufacturing ICT devices in the region. Moreover, it requires companies to hire local engineers when manufacturing such products.

These requirements are antithetical to advancing a vibrant and sustainable ICT marketplace. Many view Nigeria as a leader in the ICT space for the African Union (AU), and, if these guidelines become accepted rules of the road for the AU at large (or beyond), then it does not bode well for U.S. companies seeking to enter the African market. This poses a stark barrier for U.S. trade in the ICT economic ecosystem.

[17] NITDA, *Guidelines for Nigerian Content Development in Information and Communications Technology* (2017).

RUSSIA

Issue: Data Localization Law

Federal Law No. 242-FZ, signed by President Vladimir Putin in July of 2014, requires companies that store and process the personal data of Russian citizens to maintain servers on Russian soil and to notify the federal media regulator, Roskomnadzor, of all server locations.[18] It empowers Roskomnadzor to block websites and to maintain a registry of data violators. Additionally, in August 2015 a non-binding clarification suggesting that localization might apply to websites that include built-in Russian-language options, transact in Russian rubles, or use a Russian top-level domain such as .r.[19] The Roskomnadzor has used this law to block internet access within Russia to the website LinkedIn, for not following the data localization requirements sufficiently.[20]

In July of 2016, a package of amendments was released imposing extensive data storage requirements on telecommunications providers and companies classified as internet telecommunications services.[21] Per these changes, telecom operators must store metadata for three (3) years and internet telecoms for one (1) year, while both must retain the content for up to six (6) months. Companies will have until July 1, 2018, to begin implementing these requirements. Moreover, if the stored messages and files are encrypted, companies will be required to provide Russian state security services with decryption keys upon request. In August 2016, Russia's Federal Security Service (FSB) announced that it has the capability to obtain information necessary for decoding the electronic messaging received, sent, delivered, and (or) processed by users of the internet.[22]

[18] Russian Federation, *Federal Law No. 242-FZ*, (July 21, 2014). *Available at* https://pd.rkn.gov.ru/authority/p146/p191/.

[19] Russian Federation's Ministry of Communications and Mass Media, *Clarifying Federal Law No. 242-FZ*, (Aug. 3, 2015). *Available at* http://www.bna.com/russia-clarifies-looming-n17179934521/.

[20] https://www.insideprivacy.com/cross-border-transfers/linkedin-blocked-in-russia-following-breach-of-data-localization-laws/

[21] Russian Federation, "*Yarovaya Package" Federal Law No 374-FZ*, (July 6, 2016). *Available at* http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

[22] Federal Security Service of the Russian Federation, *Encryption Keys*, (Aug.1, 2016). *Available at* http://www.fsb.ru/fsb/science/single.htm!id=10437866@fsbResearchart.html.

Issue: Effective Prohibitions on the Use of Strong Encryption

Under Russia’s current System of Operative-Investigative Measures (SORM), Russian ISPs must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages, and web use. In 2014, SORM usage was extended to monitoring of social networks, chats, and forums, requiring their operators to install SORM probes in their networks. Further, advances of the SORM force online communications providers to provide the authorities with a means to decrypt users’ messages, a technically infeasible result when end-to-end encryption methods are used. This law presents serious issues for small business innovators seeking to enter the Russian marketplace to compete.

TURKEY

Issue: Data Localization Requirement on Companies that Process Payments

Turkey’s E-Payment Law requires the processing of e-payments occur within Turkey.[23] Even more recently, Turkey’s Banking Regulation and Supervising Industry (BDDK) initiated a policy in mid-2016 that mandates that companies locate their ICT systems in the country.[24] These data localization requirements have chilled plans that the App Association’s members have or would have to enter this important market should their app include e-payment capabilities.

[23] U.S. Dep’t of State Bureau of Economic and Business Affairs, *2016 Investment Climate Statement – Turkey* (July 5, 2016). *Available at* http://www.state.gov/e/eb/rls/othr/ics/2016/eur/254425.htm.

[24] Turkey’s Banking Regulation and Supervising Industry (BDDK), *Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493*, Official Gazette numbered 28690, (published June 27, 2013). *Available at* https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf.

The App Association appreciates the opportunity to submit these comments to the Commission's investigations, and stand ready to work with the USITC and other stakeholders to address barriers to digital trade.

Sincerely,

Brian Scarpelli
Senior Policy Counsel

Joel Thayer
Associate Policy Counsel

Emily Baker
Membership and Research Coordinator

ACT **|** The App Association
1401 K St NW (Ste 501)
Washington, DC 20005