ACT | The App Association

Testimony
of Morgan Reed
President
ACT | The App Association

on

"21st Century Trade Barriers: Protectionist Cross Border Data Flow Policies' Impact on U.S. Jobs"

before the
House Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

October 12, 2017
2123 Rayburn House Office Building

Executive Summary

App Ecosystem:
currently valued at $143 billion; $8 trillion global market for internet of things over the next decade

Chairman Latta, Ranking Member Schakowsky, and distinguished members of the Subcommittee: My name is Morgan Reed, and I serve as president of ACT | The App Association, which represents about 5,000 small business app makers and connected device companies across the globe. Our members leverage the connectivity of devices--from cars to phones to refrigerators--to produce innovations that enhance our lives.

The app ecosystem is now valued at roughly $143 billion, and represents the front end for $8 trillion in international trade annually. Impressively, the big 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 virtually all our members engage in international trade. This is what gives us a unique voice on digital trade 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 U.S. has produced a successful tech industry, 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 industry.

We see three main barriers to continued success:

- Non-tariff digital trade barriers that result from domestic policies said to be rooted in privacy, national security, law enforcement, or similar interests;
- Efforts in international forums to restrict cross-border data flows; and
- Conflicts between U.S. law enforcement agencies' access to data stored overseas and foreign laws, which could be ameliorated with legislation such as the International Communications Privacy Act (ICPA) (H.R. 3718).

7 million U.S. tech sector jobs; growth rate of tech sector:
3 percent

Digital trade supports American jobs, and it can also save lives. The future of medicine is in data and artificial intelligence. A successful physician might see about 15,000 patients throughout her career, but recent innovations in technology have grown doctors' 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 software tools, a doctor can plug in a patient's characteristics and see which medication is most likely to work. These advantages benefit everyone, and yes, they can save lives. But they can only exist when data is accessible. Our member companies know that policies that stop data at national borders seriously degrade these life-saving capabilities.

In an example this Subcommittee knows all too well, the United States faces more than 35,000 traffic fatalities every year, the majority of which are due to human error. However, with the right technological advances, lives will be saved. Airbags, safety belts, and other innovations helped reduce traffic fatalities from a high of nearly 55,000 in 1972. But the next advances in safety technology will depend on access to international data. Self-driving cars will run not just on energy, but also on data from drivers and traffic patterns from around the globe. How can a self-driving car recognize a bicycle or a cyclist? How does it know the cyclist is not a tree? The machine-learning engine that cars use must have seen bikes in all their forms, in millions of different contexts. The United States simply cannot provide all the scenarios self-driving cars will encounter, therefore American car companies, especially those that sell in overseas markets, must perform testing overseas that depends on the cross-border transfer of data. When foreign governments enact policies that encumber the flow of data overseas—some going so far as to directly require the localization of data—they are blocking U.S. companies from using a key resource, not just to create jobs, but also to save lives.

Some barriers to cross-border data flows are direct and intentional, and others are unintentional consequences of domestic priorities. We are working hard to educate foreign governments on the effects their domestic policies could have on cross-border data flows. We urge American policymakers to look to trade agreements as a tool to help ensure the policies intended to protect privacy do not unduly burden cross-border data flows and hurt U.S. job creation.

As American trade negotiators work to preserve the digital economy, Congress should consider updating key statutes to remove conflicts with other sovereign laws. Among other things, ICPA would reduce crippling legal uncertainty for our members and American companies looking to do business overseas. It would also provide cover for American trade negotiators as they seek to show foreign governments that our privacy protections are equal to theirs.

The digital economy is steadily growing more important in our trade relationships, giving rise to numerous actions by foreign interests that have serious consequences for American businesses. Many of the battles we are fighting today feel like déjà vu—they are remarkably similar to the issues this Subcommittee highlighted three years ago. As these trends continue, our trade relationships present the best opportunity to stop digital protectionism abroad and protect economic growth and job creation at home. I look forward to a discussion about how we can accomplish these goals, and working with the Subcommittee on these issues in the future.

I. American Small Business Innovators Face Numerous Barriers to the Free Flow of Data Across Borders

Foreign governments seek to encumber the free flow of data across political boundaries for many reasons and in a variety of ways. While some of these policies are based on legitimate goals (e.g., to protect privacy rights or public safety), they are often thinly veiled efforts to protect domestic industry. Previously-negotiated language to address these policies would require signatory countries to "allow the cross-border transfer of information by electronic means, including personal information . . .,"[1] one of many landmark provisions poised to assist the growth of the digital economy. The App Association continues to urge the U.S. Trade Representative (USTR) to include this clear protection of cross-border data flows in any update to the North American Free Trade Agreement (NAFTA)— to ensure American businesses in the digital economy may access the Canadian and Mexican markets more easily, and to serve as a standard for future trade agreements.

a. Frequency of Data Localization Requirements Limits U.S. Small Business Innovators' Ability to Grow

The required siting of data centers and digital infrastructure—and mandates to store data—inside of a country's borders harms the free flow of data across borders. These policies serve as a direct barrier to market access, and ignores the efficiencies of cloud computing. Previous multilateral agreement language sought to address these problematic proposals with a provision prohibiting member countries from requiring companies to "use or locate computing facilities" inside that country's borders, with limited exceptions. We support NAFTA, currently being re-negotiated between the United States, Canada, and Mexico, and encourage the inclusion of similar provisions to provide a predictable policy across North America, and a strong signal to combat the growing number of data localization policies we see around the globe.

Numerous data localization requirements are in place today, actively locking American small businesses out of important markets. Key examples include:

China has either proposed or implemented numerous restrictions on the flow of data across its borders. These regulations limit or prohibit the transfer of data related to banking and financial credit, cybersecurity, counterterrorism, commercial information systems, healthcare, and insurance outside of China. These policies each represent a significant barrier to market entry and serve as a non-starter for small businesses that would otherwise look to China to expand their businesses and create jobs.

- 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.[2] The European Centre for International Political Economy has estimated that Indonesia's use of data localization requirements, in this context and others, will result in a 0.7 percent loss in its gross domestic product.[3]
- India's National Data Sharing and Accessibility Policy requires all data collected using public funds be stored within the borders of India.[4] In addition, India's 2015 National Telecom M2M ("machine to machine") Roadmap,[5] which has not been implemented, states that all M2M gateways and application servers serving customers in India must be located within India. The draft policy also proposes rules that prohibit the use of foreign SIM cards in devices in India.
- Russia's Federal Law No. 242-FZ, signed by President Vladimir Putin in July 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.[6] This law empowers Roskomnadzor to block websites and to maintain a registry of data violators.
- Turkey's E-Payment Law mandates the processing of e-payments must occur within Turkey.[7] In mid-2016, Turkey's Banking Regulation and Supervising Industry (BDDK) initiated a policy that requires companies to locate their ICT systems in Turkey.[8] These data localization requirements have jeopardized our members' plans to enter this important market should their app include e-payment capabilities.
- Nigeria has implemented even harsher data localization policies, not only requiring companies to store their data within Nigeria, but also mandating that at least 50 percent of any information or communications technology devices manufactured in the region be comprised of locally sourced inputs.

Data localization requirements are being implemented at an alarming rate that continues to grow. Our members rely heavily on cloud computing and its efficiencies, but these policies create significant barriers and untenable burdens. The ability to use cloud service providers to store and process data has allowed our members and businesses of all sizes to compete in the global economy and reach consumers around the world. However, requiring the construction of new data centers, or the exclusive storage of data in a country, coupled with the inability to share data across borders hurts these opportunities for global engagement and success. American businesses need strong provisions in future trade agreements to combat these real and growing data localization policies. Now is a vital time for the United States to lead by example, both in domestic laws and our negotiated bilateral and multilateral trade agreements.

Similarly, our members encounter a growing number of policies that require the transfer of proprietary source code or encryption keys as a condition for market entry.[9] These policies are unacceptable for our members, and businesses of all sizes, because their intellectual property (IP) is the lifeblood of their innovation.

b. European Privacy Laws Are Particularly Burdensome for Small and Medium-Sized Companies

Some countries' policies impede the international flow of data, and business, in unintentional ways. For example, various provisions of the General Data Protection Regulations (GDPR), set to go into effect on May 25, 2018, impose additional requirements on non-European firms that increase the cost and risk associated with handling data that may pertain to EU citizens. For example, Article 27 of the pending law requires firms to physically place a representative in the EU.[10] This can be an insurmountable hurdle to our small and medium-sized members entering the EU market. Anything that can be done during GDPR implementation to ease the burden for these small and medium-sized companies could have hugely positive economic implications.

The new GDPR requirements have also created conflicting obligations for foreign companies that abide by U.S. and other international laws. For example, the impact of the GDPR on the oversight and management of the global domain name system, currently implemented by the Internet Corporation for Assigned Names and Numbering (ICANN), is uncertain. The GDPR may jeopardize ICANN's effectiveness by inhibiting the transfer of information about websites that is necessary to protect consumers and intellectual property. This is not just an impediment to U.S. companies that provide critical Domain Name System (DNS) functions, but also to the broader digital economy that depends on their services.

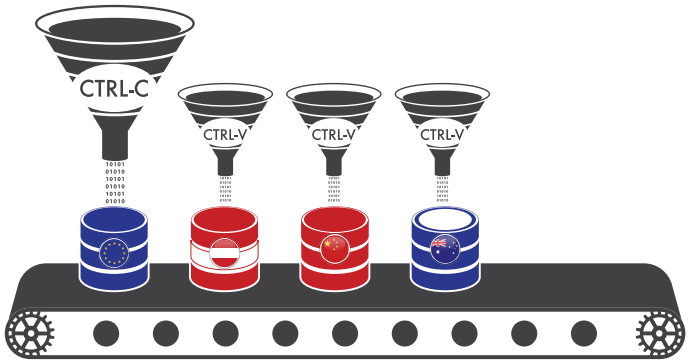
c. Privacy Shield as a Model for Protecting Data While Facilitating Data Flows

The recent trend of unilaterally imposed restrictions to cross-border data flows is damaging for businesses of all sizes. For instance, many governments are seeking to force data to reside within national boundaries by imposing data localization laws, strict licensing regimes, data retention requirements, government procurement regulations, and pressure on public sector sales. We urge policymakers to look to trade agreements as a tool to help ensure these sorts of detrimental policies do not unduly burden cross-border data flows and hurt U.S. job creation.

For example, the Privacy Shield framework between the EU and the U.S. offers a bilateral cross-border data transfer framework that could be a model for other jurisdictions concerned about protecting personal data leaving national borders.

Numerous App Association members have undertaken significant effort to meet the Privacy Shield's requirements and are today certified to the Privacy Shield. The U.S. government has also taken significant steps to hold up its end of the bargain by holding companies that certify to the Shield to account.[11]

As a result, we strongly believe the Privacy Shield provides protections that are "essentially equivalent" to those of European law, and support its continuation. The App Association has communicated this support directly to the EC at its invitation in July of 2017.[12] The first annual joint EU-U.S. review of the Privacy Shield is a landmark assessment that we are closely engaging with regulators about, on both sides of the Atlantic. Our small business members would be especially disadvantaged by the invalidation of the Privacy Shield.



II. Ongoing Efforts to Expand the Scope of the International Telecommunications Union

International governmental organizations pose unique threats to the global digital economy. The International Telecommunication Union's (ITU) proposal contemplating a role for itself in over-the-top (OTT) services is particularly concerning. An agency of the United Nations (UN), the ITU allocates global radio spectrum, manages satellite orbits, and develops technical standards to ensure the interconnection of telecommunications. However, the ITU does not currently have a role in internet traffic or services.

The ITU's Council Working Group (CWG) has proposed an "Open Consultation" to gather comments from stakeholders about public policies pertaining to OTT services.[13] In general, OTT services refer to those that operate on the internet, including apps and websites.

Numerous data localization requirements are in place today, actively locking our American small businesses out of key markets. Key examples include:

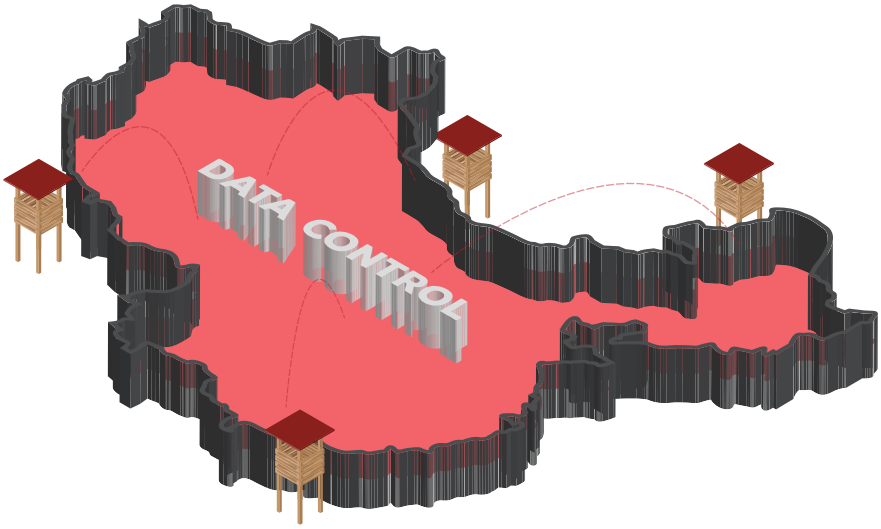
Therefore, in concert with existing laws for companies that operate on the internet, the imposition of specific regulations on OTT services would be redundant, and serve as additional barriers to trade.

While a proposal to examine public policies concerning OTT services may seem benign, a similar proposal in 2012 sought to expand the ITU's reach to include the regulation of internet services. The proposal was largely viewed as an international justification for heavy-handed regulation, partitioning, and censorship of the internet. The United States ultimately challenged the 2012 proposal during the World Conference on International Telecommunications (WCIT), and Representative Mary Bono, this Subcommittee's then-chairwoman, put forth a congressional resolution to allow the U.S. delegation to walk away from an ITU vote on the issue.[14]

The ITU's current proposal is just as threatening. Expanding ITU's reach to include OTT services would represent the UN's intervention into general online commerce policy, and could easily result in the arbitrary taxation of internet traffic on a country-by-country basis. The App Association filed detailed comments opposing the ITU's expansion into OTT services and presented our argument to ITU member state delegations in in Geneva, Switzerland, last month. We also served as a sector expert for the U.S. delegation to the ITU's working group on Internet Governance, where we reinforced these viewpoints to ITU staff and member states.

We believe the Subcommittee should closely monitor, and consider engagement in, OTT-related developments in the ITU, and vigilantly seek opportunities to bolster the U.S. bargaining position in bilateral, multilateral, and international contexts. We believe a resolution in line with Representative Bono's could help prevent mission creep at the ITU. We remain committed to working with this Subcommittee to advance U.S. interests in the ITU, and to keep the ITU's efforts within its remit.

III. Conflicts Between Domestic and Foreign Data Access Laws



Cloud computing has enabled American app developers to securely access, share, and store the 2.5 quintillion bytes of data created daily to better serve consumers across the globe. Unfortunately, the Electronic Communications Privacy Act (ECPA), the statute governing law enforcement's access to stored data, was written in 1986, long before the advent of cloud computing, and does not clearly outline when and how law enforcement can access data stored overseas. Several U.S. courts have contradicting interpretations of ECPA's reach, and many have concluded that ECPA's scope is so broad that it directly conflicts with other countries' domestic laws. While these differing legal conclusions remain unresolved, many law enforcement agencies continue to use ECPA to authorize requests for data pertaining to citizens of any country, stored in any country. As companies increasingly store data on servers around the world, this creates serious uncertainties for their operations and success.

Compliance with a law enforcement request that conflicts with domestic laws could, in some instances, result in a penalty of up to 4 percent of global revenue for a company. In these cases and others where a conflict exists between domestic and foreign law enforcement statutes,[15] our members are stuck between a rock and a hard place, or left with a significant financial burden. The confounding legal uncertainty undoubtedly establishes a non-tariff barrier to digital trade—it requires substantial capital and legal resources that small businesses like our members simply cannot bear.

Nonetheless, the App Association favors the reform of intelligence surveillance and criminal investigation statutes, and strongly believes Congress should reform ECPA. The App Association deeply appreciates the House of Representatives' unanimous passage of the Email Privacy Act (H.R. 387) earlier this year. However, more must be done to ensure U.S. companies doing business abroad do not face conflicts between law enforcement requests and foreign laws. We believe ICPA (H.R. 3718) legislation would ameliorate conflicts between foreign laws and U.S. law enforcement agencies' authority to obtain data pertaining to foreign citizens, and help remove this trade barrier.

IV. Intellectual Property Rights and Competition Law

Every year, app makers and content creators lose an estimated $3 to $4 billion from the installation of roughly 14 billion pirated apps globally.[16] Several foreign governments continue to use competition law to propose and enact policies that seek to extract, or make it hard to protect, U.S. companies' valuable intellectual property. The strong protection of IP is crucial to our members' ability to do business overseas.[17]

V. Conclusion

This Subcommittee has a strong history of bolstering digital trade priorities. We are heartened by the continued focus on these issues, but the stakes are higher today than when the Subcommittee last examined these issues three years ago. An ever-growing number of American jobs depend on digital trade, while the interests that support digital protectionism are becoming more influential. We have much more work to do to protect the vitality and dynamism of the digital economy, and we look forward to working with you in these shared endeavors.

---

1 Art. 14.11, TPP (2015) found here: https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf.

2 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.

3 http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

4 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.

5 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.

6 Russian Federation, Federal Law No. 242-FZ, (July 21, 2014), available at https://pd.rkn.gov.ru/authority/p146/p191/.

7 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.

8 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.

9 See https://actonline.org/wp-content/uploads/MIIT-Pre-Installated-App-Regulation-.pdf; http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

10 https://www.privacy-regulation.eu/en/27.htm

11 https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield

12 http://actonline.org/wp-content/uploads/07052017_App-Assn-Ltr-re-EU-US-Privacy-Shield.pdf

13 http://www.itu.int/en/council/cwg-internet/Pages/consultation-june2017.aspx

14 https://www.congress.gov/112/bills/hconres127/BILLS-112hconres127rfs.pdf

15 See http://ehoganlovells.com/cv/92a5426dc5d9947a6ef3abd4eb988b549ae2472b

16 https://www.forbes.com/sites/johnkoetsier/2017/07/24/app-developers-losing-3-4-billion-annually-thanks-to-14-billion-pirated-apps/#697b170460da

17 The App Association is advising USTR on its investigation into China's intellectual property protection policies.