October 1, 2025

Silvia Savich
Deputy Assistant U.S. Trade Representative for Russia and Eurasia
Office of the United States Trade Representative
600 17th Street NW
Washington, District of Columbia 20036

**RE: Input of ACT | The App Association regarding the U.S. Trade Representative's *Request for Comments and Notice of Public Hearing Concerning Russia's Implementation of Its WTO Commitments* (Docket No. USTR-2025-0010; 90 FR 38877)**

Dear Ms. Savich:

ACT | The App Association (App Association) writes in response to the interagency Trade Policy Staff Committee's (TPSC) request for comments to assist the Office of the United States Trade Representative (USTR) in preparing its annual report to Congress on Russia's World Trade Organization (WTO) commitments,[1] in accordance with Section 201(a) of the Russia and Moldova Jackson-Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012.[2]

The App Association is a global trade association representing small business technology companies from across the United States. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents—which we call the app economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[3]

[1] 90 FR 38877.
[2] Pub. L. 112-208.
[3] ACT | The App Association, State of the U.S. App Economy, available at https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

## I. ACT | The App Association's General Trade Priorities

The global digital economy holds great promise for small app development companies, but our members face a diverse array of trade barriers when entering new markets. These barriers may take the form of laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of particular domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights. However, they all have the same net effect: impeding U.S. exports and investment at the expense of American workers.

We support efforts by the U.S. government to protect American businesses and workers and remain committed to working with public and private sector stakeholders to ensure WTO agreements effectively reduce or eliminate trade barriers in the app economy. U.S. trade and investment partners must implement policies that embrace the realities of our global economy, and address the following trade abuses:

- ***Limiting Cross-Border Data Flows***: Limiting cross-border data flows hurts all players in the digital economy. The seamless flow of data across economies and political borders is essential to the global economy. In particular, innovative small app development companies rely on unfettered data flows to access new markets and customers.
- ***Data Localization Policies***: Companies expanding into new overseas markets often face regulations that force them to build and/or use local data infrastructure. These data localization requirements seriously hinder imports and exports, as well as jeopardize an economy's international competitiveness and undermine domestic economic diversification. Small app developers often do not have the resources to build or maintain infrastructure in every country in which they do business, which effectively excludes them from global commerce.
- ***Customs Duties on Digital Content***: American app developers and technology companies take advantage of the internet's global nature to reach the 95 percent of customers who are outside the United States. However, the "tolling" of data across political borders with the intent of collecting customs duties directly contributes to the balkanization of the internet and prevents small business digital economy innovators from entering new markets.
- ***Requirements to Provide Source Code for Market Entry:*** Some governments have proposed or implemented policies that make legal market entry contingent upon the transfer of proprietary source code. For app developers and tech companies, intellectual property is the lifeblood of their business, and the transfer of source code presents an untenable risk of theft and piracy. These requirements present serious disincentives for international trade and are non-starters for the App Association's members.

- ***Requirements for "Backdoors" in Encryption Techniques:*** Global digital trade depends on technical data protection methods and strong encryption techniques to keep users safe from harms like identity theft. However, some governments and companies insist that "backdoors" be built into encryption for the purposes of government access. 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. From a security and privacy standpoint, the viability of app developers' products depends on the trust of end users.
- ***Intellectual Property Violations***: The infringement and theft of intellectual property (IP) jeopardizes the success of App Association members and hurts the billions of consumers who rely on their app-based products and services. Each kind of IP (copyrights, trademarks, patents, and trade secrets) represents distinct utilities upon which App Association members depend. IP violations lead to customer data loss, interruption of service, revenue loss, and reputational damage – each alone is a potential "end-of-life" occurrence for a small app development company. Strong and fair protection of intellectual property for copyrights, patents, trademarks, and trade secrets is essential to their businesses.
- ***Misapplication of Consumer Protection and Competition Laws to New and Emerging Technology Markets:*** Various regulators, including key trading partners, are currently considering or implementing policies that would put mandates on nascent and developing emerging technology markets. For example, some regulators are jeopardizing small businesses' ability to compete by upending the functionality of digital platforms that lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections. Others are considering interventions into undefined and emerging technology markets, such as for artificial intelligence. Foreign governments upending technology markets through misguided regulations inconsistent with U.S. law will disadvantage American innovators and serve as significant trade barriers.

The App Association believes that addressing the trade abuses across key economies, including Russia, is critical to ensuring the United States can leverage the digital economy to create greater prosperity and opportunity for American businesses and workers. If these abuses persist, it will inevitably harm American workers and manufacturers, intellectual property rights and innovation, and research and development opportunities in our country.

## II. Specific Comments on Russia's Compliance with WTO Commitments

Accession to the WTO in 2012 brought expectations that Russia would harmonize its regulations with well-established, pro-trade policies that enable fair treatment of new market entrants. However, we do not believe that these commitments have been met. The App Association has observed a growing tendency to enact policies that discriminate against "foreign" market entrants in the digital economy. The App Association submits the following comments to give insight to these policies, which implicate Russia's adherence to its obligations under the WTO General Agreement on Tariffs and Trade (GATT) and General Agreement on Trade in Services (GATS):

- **Data localization:** Through its implementation of several laws, the Russian government has enacted policies that require the storage of data within the borders of Russia for periods of time (six months, one year, etc.), such as Federal Laws 242-FZ, 374-FZ, 375-FZ, and 149-FZ. In July 2025, amendments strengthened the requirement that personal data of Russian citizens must be collected, processed, and stored exclusively on servers located in Russia, with expanded liability for non-compliance, including higher fines and potential service blocking. These requirements extend beyond large multinationals to small and medium foreign firms, raising entry barriers. The Russian government claims these laws are meant to be used to quell terrorism, but the ramifications are felt economy-wide, particularly in Russia's digital economy. The data retention requirements are far broader than other countries, encapsulating "voice data, text messages, pictures, sounds, and video, not just the metadata."[4] While some large companies may have the ability to reach one-off deals to gain market access, these policies present an insurmountable barrier to entry for the small business software developer community the App Association represents. To implement these policies, many companies are forced to raise prices two- to three-fold to cover the cost, burdening consumers and dragging down the economy.[5] Further, Russia has taken enforcement actions against select companies, sending a chill across the business environment, and particularly small business digital economy innovators, discouraging any plans to bring new innovations to the economy.[6]
- **Mandates to weaken technical protection mechanisms, which hurt end-user privacy and customer trust:** Small business app companies depend on customer

[4] Nigel Cory, "The Worst Innovation Mercantilist Policies of 2016," Information Technology & Innovation Foundation (January 2017), *available at* https://www2.itif.org/2017-worst-innovation-mercantilist-policies.pdf?_ga=2.130966605.31642201.1632150946-570963714.1631032712.

[5] Laura Mills, "New Russian Data Laws Worry Rights Activists, Telecom Companies," The Wall Street Journal, July 7, 2016, http://www.wsj.com/articles/new-russian-data-laws-worry-rights-activists-telecomcompanies-1467905452.

[6] TechCrunch, "Russia says 'nyet,' continues LinkedIn block after it refuses to store data in Russia" (May 7, 2017), *available at* https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/.

trust to grow and create jobs. This trust can only be maintained by utilizing the strongest technical protection mechanisms available, including encryption. The Russian government has enacted laws that require companies to store data locally and provide encryption keys to relevant Russian authorities. Telecommunication companies and internet service providers are directed to disconnect services to their users if they do not acquiesce to Russian law enforcement's "request" for verification of their identity, implicating various privacy concerns.[7] The Russian government's practices reach American companies by placing them into a broadly-defined category of telecom providers and "facilitators of information dissemination by means of the internet," including online messaging services, email providers, social media, and voice over internet protocol services (which use the internet to transmit voice and multimedia).[8] For example, Russian law requires apps to provide their users' phone numbers to the government. While this is done under the veil of safety for citizens, it restricts the free flow of information and serves as a trade barrier. In addition to existing requirements, Russia has expanded its ability to compel disclosure of encryption keys and user identifiers, while simultaneously criminalizing certain circumvention tools. As of July 2025, individuals may be fined for merely searching for content labeled "extremist," even when accessed unintentionally via VPN. This escalation further erodes privacy protections and chills both consumer trust and market access for foreign digital services.

Moreover, Russia enacted regulations that prohibit consumers' ability to use virtual private networks (VPNs) to access websites as an anonymous browser in 2017. The 2017 VPN restrictions remain in force, and enforcement has intensified; in 2025, new penalties expanded in scope so that individuals now face liability for searching or attempting to access prohibited content via VPN. Internet service providers and platforms that fail to block access are subject to loss of market access and heavy fines. The Russian government cites this regulation as an effort to keep people from accessing dangerous and illegal content. This regulation says that any internet providers that allow these to exist, or function without being blocked, will lose their market access.

- **Domain name system (DNS) manipulation:** Enacted in May 2019, Federal law N90-FZ enables the Russian government to create an alternative national DNS to enable greater government control of internet traffic within Russia.[9] Since the 2019 adoption of Federal Law N90-FZ, Russia has taken further steps to centralize DNS control, continuing to develop a parallel national DNS infrastructure and

[7] *Id*.

[8] "New Russian Legislation on Massive Telecoms Surveillance," Jones Day Publications (July 2016), http://www.jonesday.com/new-russian-legislation-on-massive-telecoms-surveillance-07-12-2016/.

[9] How Russia is Stepping Up Its Campaign to Control the Internet, TIME (Apr. 1, 2021), https://time.com/5951834/russia-control-internet/.

increasingly mandating use by state institutions and certain private entities, raising concerns about digital fragmentation and further state control of internet traffic. The App Association has significant concerns with such efforts aimed at undermining the global open DNS that enables data flows necessary for the app economy's sustainability and growth.

- **Pre-sale app installation requirements:** As of 2021, Russian law requires the installation of Russian software on various certain consumer electronic products before sale in the country.[10] The 2021 pre-installation requirement remains in place, with enforcement since expanding to additional device categories and the Ministry of Digital Development introducing updated lists of mandatory domestic apps in 2024–25. These updates further entrench state-preferred digital ecosystems while disadvantaging foreign software providers. By requiring the pre-installation of Russian software on various information and communication technology (ICT) products, Russia positions itself to discriminate against "foreign" apps from competing in the Russian market and may undermine security on such devices. This requirement negatively impacts the integrity of both the manufacturer and internet service provider platforms, as well as the larger app ecosystem.

The App Association appreciates the opportunity to submit these comments to the TPSC.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

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

[10] Russia Passes Law Forcing Manufacturers to Install Russian-made Software, THE VERGE (Dec. 3, 2019), https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphoneslaptops.