Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act

Vendors from the U.S. and allied countries have supplied the world's information communications and technology (ICT) for decades. In recent years, the global ICT supply chain has changed dramatically; a number of prominent foreign vendors – many subject to the control of autocratic and illiberal governments – have gained significant market share in a variety of internet infrastructure, online communications, and networked software markets. The growth and prevalence of these untrusted vendors pose serious risks to the nation's economic and national security.

The RESTRICT Act comprehensively addresses the ongoing threat posed by technology from foreign adversaries by better empowering the Department of Commerce to review, prevent, and mitigate ICT transactions that pose undue risk, protecting the US supply chain now and into the future.

THE CHALLENGE:

Over the past years, foreign technology, including telecommunications equipment, social media applications, security software, and e-commerce platforms, have entered the U.S. market and become increasingly embedded within our information and communications networks, posing novel threats to U.S. citizens' data, U.S. critical infrastructure, the privacy of Americans' and businesses' communications, our information ecosystem, and security of everyday products.

Notable ICT products – such as Kaspersky antivirus software, telecommunications equipment supplied by Huawei, and software products from firms based in the People's Republic of China (PRC) – gained traction while the United States government struggled to identify and respond to threats posed by these products in a timely manner. Growing concerns with consumer software from vendors in the PRC – such as ByteDance's TikTok, Tencent's WeChat, and Alibaba's Alipay – have raised serious concerns about a lack of consistent policies to identify threats posed by foreign ICT products and insufficient authorities to act decisively and comprehensively to address them. Further illuminating these concerns, the top two apps by absolute downloads in the United States from January 15, 2023 to February 13, 2023 were from PRC vendors Temu and ByteDance.

Individual agencies have attempted to utilize their various authorities to address foreign ICT threats within their own jurisdictions, but efforts have often been disjointed, failed to comprehensively address identified risks, or, simply proved slow and under-suited to the complexity and interconnectedness of the global ICT supply chain. Further, these efforts often rely on antiquated authorities delegated to the President by Congress in a pre-digital age.

A new approach is needed to systemically review and address the challenges posed by technology from foreign adversaries. Both the current and previous Administrations have rallied around a more holistic solution: granting the Department of Commerce authority to review, block, and mitigate a range of transactions involving foreign information and communications technology that pose undue risk.

THE SOLUTION:

The RESTRICT Act establishes a risk-based process, tailored to the rapidly changing technology and threat environment, by directing the Department of Commerce to identify and mitigate foreign threats to information and communications technology products and services.

This measured, risk-based approach is especially vital in the context of personal communications services, where federal courts have blocked prior efforts to take remedial steps against foreign software vendors as insufficiently tailored and based on insufficiently-substantiated risks.

The *Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act* would:

- Require the Secretary of Commerce to establish procedures to identify, deter, disrupt, prevent, prohibit, and mitigate transitions involving information and communications technology products in which any foreign adversary has any interest and poses undue or unacceptable risk to national security.
- Prioritize evaluation of ICT products used in critical infrastructure, integral to telecommunications products, or pertaining to a range of defined emerging, foundational, and disruptive technologies with serious national security implications.
- Ensure comprehensive actions to address risks of untrusted foreign ICT by requiring the Secretary to take up consideration of concerning activity identified by other USG entities.
- Educate the public and business community about the threat by requiring the Secretary of Commerce to coordinate with the Director of National Intelligence to provide declassified information on how transactions denied or otherwise mitigated posed undue or unacceptable risk.