Limitations on Cryptography Rulemaking in Trade Agreements Could Generate Cybersecurity Risks and Create Unwarranted New Secrecy Rights for Corporations

During the last decade, some trade agreements have ventured into rulemaking on deeply technical aspects of communications, information, and digital policy. Often in response to tech industry lobbying, negotiators have included binding commitments in trade agreements setting limits on governments' ability to regulate myriad matters, such as online privacy, algorithmic accountability and artificial intelligence, competition policy, and taxation. The trade-pact provisions associated with these policy domains have received considerable attention during recent years, prompting countries to reassess their positions on data flows and storage, software secrecy guarantees, "non-discrimination for digital products," and liability shields for platforms that have been included, typically, in "e-commerce" or "digital trade" chapters.

A lesser-known rule that has made its way to a handful of trade agreements establishes limits on what countries can do in terms of regulation related to the use of cryptography by information and communication technology (ICT) products. Indeed, a **term that was included in the Trans-Pacific Partnership[1], which after the U.S. decision to exit the deal was renamed Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), and in the U.S.-Mexico-Canada Agreement[2] (USMCA) limits certain policies that countries might desire to adopt with respect to cryptography.** A similar rule has been proposed in the context of the Joint Statement Initiative (JSI) on E-commerce currently being negotiated by a subset of members of the World Trade Organization (WTO).[3]

Broadly, this term prohibits governments from requiring firms operating in their territory to:

(i) transfer or provide access to any proprietary information relating to cryptography, for example, a private key, algorithm specifications, or other design details;

(ii) partner or otherwise cooperate with a person in its territory; or

(iii) use or integrate a particular cryptographic algorithm.

Government access to information related to cryptography, particularly when it comes to private communications and "traceability" requirements, is a sensitive topic. Human rights defenders are rightly concerned about national security or law enforcement authorities abusing their powers to unduly access private communications. In that sense, **the prohibition related to government requests to disclose cryptographic information could be justifiable. Yet these**

[1] Trans-Pacific Partnership, Annex 8-B, Section A.
[2] US-Mexico-Canada Agreement, Annex 12.C, Article 12.C.2.
[3] WTO ELECTRONIC COMMERCE NEGOTIATIONS, DRAFT CHAIR'S TEXT, 21 February 2024 Revision, Art. 22. Available at: https://www.bilaterals.org/?wto-electronic-commerce-49953.

provisions include a broad exception that basically exempts requests for encrypted or unencrypted communications from national security or law enforcement authorities. Hence, these agencies' ability to access private communications remains unencumbered by the trade-pact "ITC products that use cryptography" rule. So, what would be the consequences of this rule?

It is worth considering how these clauses could limit the regulatory capacity of governments by granting firms overly broad secrecy guarantees and banning policies that countries might desire to adopt for public-interest reasons.

The ban on governments' ability to establish conditions on the type of cryptographic algorithms that firms should use, even if such conditions aim at ensuring system security, is especially problematic.

In order to understand the risks of such limitations, it is useful to consider the case of *post-quantum cryptography*. In recent years, there has been a substantial amount of research on quantum computers – machines based on quantum physics that would be able to solve mathematical problems too difficult or intractable for conventional computers.[4] If or when large-scale quantum computers are built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.[5]

Cognizant of this security risk, in 2022 the Biden administration launched a whole-of-government strategy to "promote United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems." The objective of this strategy is to kickstart the transition to interoperable quantum-resistant cryptography by 2035. In order to meet this objective, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) are each developing technical standards for quantum-resistant cryptography. According to the presidential memo, once these standards have been developed, NIST and other governmental agencies are to establish a plan requiring agencies to upgrade their IT systems to quantum-resistant cryptography.[6] Moreover, in the case of national security systems, the President already has ordered agencies to implement enhanced cryptographic systems, namely those with symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions).[7] In order to do so, agencies will likely require IT providers to adopt the new technologies. **Such requirements to upgrade to interoperable quantum-resistant cryptography are likely to run afoul the obligation included in the trade-pact term**

[4] https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html
[5] https://csrc.nist.gov/projects/post-quantum-cryptography/.
[6] Sec. 3 (viii). Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.
[7] Sec. 3 (xiv). Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

that bans governments from requiring the use or integrate a particular cryptographic algorithm.[8]

Paradoxically, while the specific exception included in this provision would permit national security and law enforcement agencies to require access to encrypted and unencrypted communications despite potential human rights concerns of such demands, governments trying to improve cryptographic systems' integrity and security are not provided an equivalent exception, at least in the context of the E-commerce JSI. The latest known draft of the JSI text copies verbatim the security exceptions of the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS),[9] which only apply in the context of limited, explicitly enumerated circumstances that may not provide a justification for governments requiring improved cryptographic system integrity and security.

The case of post-quantum encryption provides just one example of the perils associated with tying policymakers' hands through binding and nearly unamendable trade agreements as the technological frontier progresses and generates new regulatory needs.

[8] It is unclear whether establishing general application conditions for government procurement falls within the narrow definition that WTO agreements have often adopted of this term. In the case of CPTPP and USMCA, the ICT Products that Use Cryptography is not covered by a general carveout of government procurement.

[9] WTO ELECTRONIC COMMERCE NEGOTIATIONS, DRAFT CHAIR'S TEXT, 21 February 2024 Revision, Art. 5. Available at: https://www.bilaterals.org/?wto-electronic-commerce-49953.