2. To that end, other than as provided in paragraph 4, neither Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created or developed the information.[15]

3. Neither Party shall impose liability on a supplier or user of an interactive computer service on account of:

(a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or

(b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable.

4. Nothing in this Article shall:

(a) apply to any measure of a Party pertaining to intellectual property, including measures addressing liability for intellectual property infringement; or

(b) be construed to enlarge or diminish a Party's ability to protect or enforce an intellectual property right; or

(c) be construed to prevent:

(i) a Party from enforcing any criminal law; or

(ii) a supplier or user of an interactive computer service from complying with a specific, lawful order of a law enforcement authority.

Article 19
Cybersecurity

1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:

(a) build the capabilities of their respective competent authorities responsible for computer security incident response; and

(b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.

2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its territory to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

Article 20
Open Government Data

1. The Parties recognize that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation.

2. To the extent that a Party chooses to make government information available to the public, it shall endeavor to ensure that the government information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed.

3. The Parties shall endeavor to cooperate to identify ways in which each Party can expand access to and use of government information that the Party has made public, with a view to enhancing and generating business opportunities, especially for small and medium-sized enterprises.

Article 21
Information and Communication Technology Goods
that Use Cryptography

1. For the purposes of this Article:

(a) "cipher" or "cryptographic algorithm" means a mathematical procedure or formula for combining a key with plaintext to create a ciphertext;

[15] For greater certainty, a Party may comply with this Article through its laws or regulations or through existing legal doctrines applied through judicial decisions.