119TH CONGRESS
2D SESSION

S. _____

To establish the applicability of antitrust laws to the sharing of artificial intelligence frontier model risks, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. SCHIFF (for himself and Mr. BANKS) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish the applicability of antitrust laws to the sharing of artificial intelligence frontier model risks, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Collaboration on Adversarial Threats and Security Risks Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) ANTITRUST LAWS.—

(A) IN GENERAL.—The term ''antitrust laws'' has the meaning given that term in sec-

tion 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(B) RULE OF CONSTRUCTION.—For the purposes of this Act, the laws described in section 102(2) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(2)) are consistent to the extent they do not conflict.

(2) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given that term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 4001 note).

(3) ASSISTANCE.—The term ''assistance'' includes the provision of software, hardware, data, personnel, and other resources.

(4) ASSISTANT ATTORNEY GENERAL.—The term ''Assistant Attorney General'' means the Assistant Attorney General in charge of the Antitrust Division of the Department of Justice.

(5) COVERED ARTIFICIAL INTELLIGENCE SECURITY PURPOSE.—The term ''covered artificial intelligence security purpose'' means the purpose of protecting against, identifying, evaluating, testing, analyzing, preventing, investigating, or mitigating a covered artificial intelligence security risk.

(6) COVERED ARTIFICIAL INTELLIGENCE SECURITY RISK.—The term ''covered artificial intelligence security risk'' means the potential for artificial intelligence, including during development, training, testing, evaluation, deployment, use, or release, to do 1 or more of the following:

(A) Be stolen, distilled, weaponized, trained, developed, or deployed by a covered nation (as defined in section 4872(f)(2) of title 10, United States Code) or an entity owned, controlled, or directed by a covered nation in a manner that poses a significant threat to the national security, including through covert, clandestine, undisclosed, or otherwise concealed development activities that attempt to evade detection or verification.

(B) Substantially facilitate the development or deployment of a chemical, biological, radiological, nuclear, or offensive cyber weapon.

(C) Cause a disruption to, degradation of, impairment of, or loss of operational control over critical infrastructure that is reasonably likely to result in a significant impact on security, national public health or safety, or any combination thereof.

(D) Substantially reduce the ability of a developer, deployer, owner, operator, user, evaluator, auditor, Federal department or agency, or other governmental authority to oversee, evaluate, monitor, control, contain, restrict access to, disable, or terminate such artificial intelligence, if the applicable person or governmental authority has authority or responsibility to do so, including through unauthorized, deceptive, evasive, or malicious activity involving such artificial intelligence.

(E) Autonomously improve, or substantially facilitate the autonomous improvement of, the capabilities of artificial intelligence in a manner that creates a substantial risk of a consequence described in subparagraph (A), (B), (C), or (D).

(F) Be vulnerable to unauthorized access that—

(i) creates a substantial risk of a consequence described in subparagraphs (A) through (E); or

(ii) is for the benefit of, at the direction of, or under the control of—

(I) a covered nation (as defined in section 4872(f)(2) of title 10, United States Code); or

(II) an entity owned, controlled, or directed by a covered nation.

(7) EXCLUSIVE PURPOSE.—The term ''exclusive purpose'', with respect to an action, means for the purpose of, with not more than an insubstantial part of the relevant action being for other purposes.

(8) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' has the meaning given that term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(9) UNAUTHORIZED ACCESS.—The term ''unauthorized access'' with respect to artificial intelligence—

(A) means unauthorized access or use of artificial intelligence; and

(B) includes—

(i) extraction or copying of model weights, parameters, or other nonpublic model information;

(ii) systematic querying or automated extraction designed to distill, replicate, or reconstruct model capabilities; and

(iii) compromise affecting the integrity, reliability, or security of artificial intelligence, including through malicious code, a backdoor, manipulated data, or compromise of an artificial intelligence model, training dataset, or artificial intelligence component.

SEC. 3. ANTITRUST EXEMPTION.

(a) IN GENERAL.—It shall not be considered a violation of any provision of the antitrust laws for—

(1) 2 or more non-Federal entities to provide or exchange information or assistance relating to a covered artificial intelligence security risk in good faith for the exclusive purpose of a covered artificial intelligence security purpose; or

(2) 2 or more non-Federal entities to coordinate or enter into agreements for the exclusive purpose of reducing covered artificial intelligence security risks via delaying or otherwise limiting the release, deployment, use, development, training, testing, or evaluation of artificial intelligence, provided that the non-Federal entities submit to the Assistant Attorney General, before undertaking the proposed coordinated delay or limitation, written notice detailing the

specific covered artificial intelligence security risk and the scope of the proposed restriction.

(b) LIMITATION.—Subsection (a) shall not apply to a non-Federal entity receiving information or assistance unless the non-Federal entity uses such information or assistance for a covered artificial intelligence security purpose and has implemented reasonable internal controls to limit the extent to which such information or assistance can be used for other purposes.

(c) AFFIRMATIVE DEFENSE.—In any action or proceeding brought under the antitrust laws, the exemption provided under subsection (a) shall constitute an affirmative defense, and any non-Federal entity claiming the exemption shall bear the burden of proving by a preponderance of the evidence that the entity's actions were taken in good faith and for the exclusive purpose described in subsection (a).

(d) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—Subsection (a)(1) shall not be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information.

(2) PRIVATE RIGHT OF ACTION.—Nothing in this Act shall be construed as limiting any private

right of action with respect to any violation of the antitrust laws that is not exempt under this section.

(e) EXEMPTION FROM DISCLOSURE.—Any information submitted to the Assistant Attorney General pursuant to subsection (a)(2), including any written notice submitted under that subsection and any information derived from such submission that would reveal the substance of such submission, shall be—

(1) used solely for the purpose of section 4;

(2) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code; and

(3) withheld, without discretion, from the public under section 552(b)(3) of title 5, United States Code.

SEC. 4. INJUNCTIVE RELIEF.

(a) IN GENERAL.—The Attorney General may seek, in a court of competent jurisdiction, an injunction against the non-Federal entities described in section 3 to prohibit an action that violates the antitrust laws.

(b) NO IMMUNITY OR EXEMPTION.—In any action described in subsection (a), this Act shall not be construed to create any immunity or exemption from injunctive relief if—

(1) the non-Federal entities do not satisfy the burden of proof under section 3(c); or

(2) the Attorney General demonstrates that, notwithstanding the covered artificial intelligence security purpose, the actions are reasonably likely to result in an overall increase in covered artificial intelligence security risks.