116TH CONGRESS
1ST SESSION

H. R. ______

To establish a national commission on online platforms and homeland security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. THOMPSON of Mississippi introduced the following bill; which was referred to the Committee on ________________

A BILL

To establish a national commission on online platforms and homeland security, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,
3 SECTION 1. SHORT TITLE.
4 This Act may be cited as the “National Commission
5 on Online Platforms and Homeland Security Act”.
6 SEC. 2. NATIONAL COMMISSION ON ONLINE PLATFORMS
7 AND HOMELAND SECURITY.
8 (a) ESTABLISHMENT OF COMMISSION.—There is es-
9
Homeland Security (referred to in this section as the “Commission”).

(b) PURPOSES.—The Commission shall—

(1) identify, examine, and report on the ways, if any, that online platforms have been utilized in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and

(2) identify, examine, and report on the ways, if any, that free speech, privacy, civil rights, and civil liberties are impacted by—

(A) any utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and

(B) any policies, procedures, or activities undertaken by owners and operators of online platforms to prevent or limit the utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and

(3) develop recommendations, as appropriate, for how online platforms could address the utiliza-
tion identified pursuant to paragraph (1), if any, in ways that are transparent and accountable, to promote free speech and innovation on the internet, preserve individual privacy, civil rights, and civil liberties, and uphold the principles of the Constitution, in accordance with relevant existing statutes, including section 552a of title 5, United States Code (commonly referred to as the Privacy Act of 1974), and take into account current or anticipated trends and technological developments, such as advancements in artificial intelligence.

(c) COMPOSITION OF COMMISSION.—

(1) MEMBERS.—The Commission shall be composed of 12 members, of whom—

(A) two members shall be appointed by the Committee on Homeland Security in the House of Representatives, with one member selected by the Chair and the other selected by the Ranking Member;

(B) two members shall be appointed by the Committee on Foreign Affairs in the House of Representatives, with one member selected by the Chair and the other selected by the Ranking Member;
(C) two members shall be appointed by the Committee on Energy and Commerce in the House of Representatives, with one member selected by the Chair and the other selected by the Ranking Member;

(D) two members shall be appointed by the Committee on Homeland Security and Government Affairs in the Senate, with one member selected by the Chair and the other selected by the Ranking Member;

(E) two members shall be appointed by the Committee on Foreign Relations in the Senate, with one member selected by the Chair and the other selected by the Ranking Member; and

(F) two members shall be appointed by the Committee on Commerce, Science, and Transportation in the Senate, with one member selected by the Chair and the other selected by the Ranking Member.

(2) QUALIFICATIONS.—

(A) AREAS OF EXPERTISE.—Individuals appointed to the Commission shall be United States persons with experience in such professions as privacy, civil rights, civil liberties, computer science and engineering, digital media
and communications, online platform management, cybersecurity, information operations, and national security. The appointment of members to the Commission shall, to the extent possible, be coordinated among nominations to ensure Commission membership represents a variety of expertise in such fields.

(B) Privacy, civil rights, and civil liberties.—Not fewer than four individuals appointed to the Commission shall be experts in the fields of privacy, civil rights, or civil liberties.

(C) Non-government appointees.—An individual appointed to the Commission may not be an officer or employee of the Federal Government.

(D) Non-industry appointees.—An individual appointed to the Commission may not be a current officer, employee, contractor, or active or significant shareholder of an entity that owns or operates an online platform.

(3) Deadline for appointment.—Members of the Commission shall be appointed not later than 30 days after the date of the enactment of this Act.
(d) CHAIR.—The Chair shall be chosen from among the members appointed to the Commission on the basis of their qualifications with respect to privacy, civil rights, and civil liberties, through a vote taken by a majority of Commission members or, in the absence of a majority, by a plurality of Commission members.

(e) INITIAL MEETING.—The Commission shall meet and begin operating not later than 30 days after the date of the appointment of its final member.

(f) QUORUM; VACANCIES.—After its initial meeting, the Commission shall meet upon the call of the Chair or a majority of its members. Nine members of the Commission shall constitute a quorum, and members shall have the option to vote by proxy. Any vacancy in the Commission shall not affect its powers, but shall be filled in the same manner in which the original appointment was made.

(g) STUDY AREAS.—The Commission shall, consistent with the purposes specified in subsection (b), analyze existing research that relates to the utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, identify any areas with respect to which additional research is needed, and study the following:
(1) The extent to which owners or operators of online platforms have been able to respond effectively to attempts to use online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, and what impact, if any, such responses have had on the privacy, civil rights, or civil liberties of users.

(2) The ways, if any, that online platforms’ algorithms or other automated decision-making systems may impact privacy, civil rights, or civil liberties, as well as how such algorithms may affect activity on online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns.

(3) The extent to which owners or operators of online platforms have transparent, consistent, and equitable policies and procedures to enforce terms of services or codes of conduct, provide notice and an opportunity for redress, or otherwise address violations of platform rules, including a consideration of best practices for improving online platforms’ policies and procedures, including the recommendations contained in the Santa Clara Principles on Trans-
transparency and Accountability in Content Moderation,
as published on February 2, 2018, or successor prin-
ciples with respect to the extent and impact of con-
tent removals and user suspensions and removals, as
well as principles related to the notice and appeals
of such decisions.

(4) The extent to which owners or operators of
online platforms consistently and effectively enforce
the policies and procedures described in paragraph
(3).

(5) The extent to which owners or operators of
online platforms consider the potential use of online
platforms in furtherance of targeted violence, includ-
ing domestic terrorism and international terrorism,
or covert foreign state influence campaigns, when
evaluating whether to enter into partnerships, adver-
tising agreements, or other business opportunities.

(h) **POWERS OF COMMISSION.**—

(1) **HEARINGS AND EVIDENCE.**—For the pur-
pose of carrying out this section, the Commission
may—

(A) hold such hearings and sit and act at
such times and places, take such testimony, re-
ceive such evidence, and administer such oaths,
(B) require, by subpoena authorized by the majority vote of the Commission, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, and documents, as the Commission may determine advisable.

(2) LIMITATIONS ON SUBPOENA AUTHORITY.—

With respect to the subpoena authority granted in paragraph (1)(B), the Commission—

(A) may only issue a subpoena to an owner or operator of an online platform;

(B) may not, under any circumstances, issue a subpoena for information related to an individual user or group of users;

(C) may not share, disclose, publish, or transmit in any way any information obtained through subpoena to a Federal department or agency, any agency of a State, local, Tribal, or territorial government, or any international body;

(D) may not share, disclose, publish, or transmit in any way any information obtained through subpoena with any individual or organization outside the Commission unless three-fourths of Commission members approve such
action and that and that any such sharing, disclosure, publishing, or transmission be reasonably necessary to further the Commission’s goals; and

(E) shall comply with requirements for the issuance of a subpoena issued by a United States district court under the Federal Rules of Civil Procedure.

(3) Public meetings and release of public versions of reports.—

(A) In general.—The Commission shall—

(i) hold public hearings and meetings, as appropriate;

(ii) hold closed or classified hearings or meetings, as appropriate;

(iii) provide an opportunity for public comment, including sharing of research and policy analysis, through publication in the Federal Register of a solicitation for public comments during a period to last not fewer than 45 days; and

(iv) release a public version of the report required under subsection (k)(2).
(B) CONDUCT.—Any public hearing, meeting, or reporting of the Commission under this paragraph shall be conducted in a manner consistent with the protection of information provided to or developed for or by the Commission as required by any applicable statute, regulation, or Executive order.

(4) OBLIGATION TO PROTECT PERSONAL INFORMATION.—Whether or not the Commission receives personally identifiable information through the exercise of subpoena authority pursuant to paragraph (1)(B), neither the Commission nor any member of the Commission may publish, disclose, or release such information publicly or to a Federal department or agency, an agency of a State, local, Tribal, or territorial government, any international body, or any other individual or organization outside the Commission.

(5) OBLIGATION TO PROTECT PROPRIETARY INFORMATION.—In the event that the Commission determines that information received from an owner or operator of an online platform includes confidential business information, a trade secret, or other proprietary information, the Commission shall ensure such information is not published, disclosed, or released.
to any individual or organization outside the Commission.

(6) Coordination with and assistance to the Under Secretary for Science and Technology of the Department of Homeland Security.—The Commission may, to the extent practicable—

(A) consult with the Under Secretary for Science and Technology of the Department of Homeland Security on the research conducted in accordance with section 3; and

(B) provide assistance in furtherance of such research, as appropriate.

(7) Personally identifiable information.—In providing testimony or producing books, records, correspondence, memoranda, papers, documents, or any other information or materials to the Commission, either to comply with a subpoena issued under this subsection or for any other purpose, owners or operators of online platforms should review such information or materials for personally identifiable information and should remove such information.

(i) Staff of Commission.—The Chair, in consultation with the Vice Chair, and in accordance with rules
agreed upon by the Commission, may appoint and fix the compensation of a staff director and such other personnel as may be necessary to enable the Commission to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(j) Security Clearances for Commission Members and Staff.—The heads of appropriate Federal departments and agencies shall cooperate with the Commission in expeditiously providing to Commission members and staff appropriate security clearances to the extent practicable pursuant to existing procedures and requirements, including temporary security clearances, as appropriate. No person may be provided access to classified information under this section without the appropriate security clearance.

(k) Reports of Commission; Termination.—

(1) Interim reports.—Not later than one year after the first meeting of the Commission, the
Chair shall report to Congress on the activities of
the Commission and share interim findings, as have
been agreed to by a majority of Commission mem-
bers.

(2) Final report.—Not later than two years
after the first meeting of the Commission, the Chair
shall submit to the President and Congress a report
that contains any findings and recommendations
agreed to by a majority of Commission members to
address the areas of study under subsection (g), in-
cluding relating to the following:

(A) Policy mechanisms that would address
the Commission’s findings in a manner that
promotes free speech and innovation on the
internet, preserves individual privacy, civil
rights, and civil liberties, and upholds the prin-
ciples of the Constitution.

(B) Policies and procedures that owners or
operators of online platforms could implement
to address such areas of study that preserve the
individual privacy, civil rights, and civil liberties
of online platform users.

(C) Mechanisms to improve transparency
and accountability related to the matters de-
scribed in subsection (g), including any best
practices identified pursuant to paragraph (3) of such subsection.

(D) Areas with respect to which additional research is required, informed by the evaluation of prior research, as required under subsection (g).

(E) Other matters identified by the majority of Commission members.

(3) TERMINATION.—The Commission shall terminate on the date that is 90 days after the date on which the final report under paragraph (2) is submitted.

(l) ACTION PLAN.—Not later than 180 days after submission of the final report of the Commission pursuant to paragraph (2) of subsection (k), the Secretary of Homeland Security shall issue an action plan in response to findings and recommendations under subparagraph (D) of such paragraph.

(m) PAPERWORK REDUCTION ACT EXEMPTION.—Subchapter I of chapter 35 of title 44, United States Code, shall not apply to this section.

(n) RULE OF CONSTRUCTION.—Nothing in this section may be construed to confer any authority, including law enforcement authority, beyond that which is authorized under existing law.
SEC. 3. RESEARCH.

(a) IN GENERAL.—The Under Secretary for Science and Technology of the Department of Homeland Security shall—

(1) analyze existing research regarding previous acts of targeted violence, including domestic terrorism or international terrorism;

(2) carry out research to better understand whether any connection exists between the use of online platforms, particularly platforms used for social media and social networking, and targeted violence, including domestic terrorism and international terrorism, that takes into consideration how the organization, structure, and presentation of information on an online platform contributes, or does not contribute, to acts of targeted violence, including domestic terrorism or international terrorism; and

(3) develop voluntary approaches that could be adopted by owners and operators of online platforms to address research findings under paragraph (2), while preserving the individual privacy, civil rights, and civil liberties of users..

(b) PARTNERSHIP.—In carrying out this section, the Under Secretary for Science and Technology of the Department of Homeland Security shall, to the extent practicable, coordinate with the National Commission on On-
line Platforms and Homeland Security under section 2, as well as academic institutions, non-profit organizations, the private sector, and Federal, State, local, and Tribal partners, as appropriate.

(c) REPORT.—Not later than one year after the date of the enactment of this section, the Under Secretary for Science and Technology of the Department of Homeland Security shall submit to Congress a report related to the research and development required under subsection (a).

(d) PAPERWORK REDUCTION ACT EXEMPTION.—Subchapter I of chapter 35 of title 44, United States Code, shall not apply to this section.

SEC. 4. DEFINITIONS.

In this Act:

(1) COVERT FOREIGN STATE INFLUENCE CAMPAIGNS.—The term “covert foreign state influence campaigns” means the coordinated and covert application of state diplomatic, informational, military, economic, business, corruption, educational, or other capability by foreign state actors to the United States to affect elections in the United States.

(2) DOMESTIC TERRORISM.—The term “domestic terrorism” has the meaning given such term in section 2331 of title 18, United States Code.
(3) INTERNATIONAL TERRORISM.—The term “international terrorism” has the meaning given such term in section 2331 of title 18, United States Code.

(4) ONLINE PLATFORM.—

(A) IN GENERAL.—The term “online platform” means internet-based information services consisting of the storage and processing of information by and at the request of a content provider and the dissemination of such content to third parties.

(B) EXCLUSIONS.—Such term does not include the following:

(i) Platforms that offer journalistic or editorial content (not including editorial decisions by online platforms to rank and organize third party content).

(ii) Applications and functionalities that enable private communications, such as email, direct messages, and encrypted communication services.

(iii) Online service providers at layers of the internet infrastructure other than the application layer, and cloud IT infrastructure service providers.
19

(5) PERSONALLY IDENTIFIABLE INFORMATION.—The term “personally identifiable information” means any information about an individual elicited, collected, stored, or maintained by an agency or owner or operator of an online platform, including the following:

(A) Any information that can be used to distinguish or trace the identity of an individual, such as a name, a social security number, a date and place of birth, a mother’s maiden name, or biometric records.

(B) Any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information.

(6) TARGETED VIOLENCE.—The term “targeted violence” means any incident of violence in which an attacker selects a particular target prior to the incident of violence so as to suggest an intent to inflict mass injury or death and may be an act of domestic terrorism or international terrorism, or an attack that otherwise lacks a clearly discernible political or ideological motivation, such as the June 12, 2016, nightclub mass shooting in Orlando, Florida, the October 1, 2017, attack on concert-goers at a music
festival in Las Vegas, Nevada, and the August 3, 2019, mass shooting at a store in El Paso, Texas.