At the end of title VII, add the following new section:

SEC. 3. REPORT ON USE BY INTELLIGENCE COMMUNITY OF FACIAL RECOGNITION TECHNOLOGY.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) the use of facial recognition technology for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion, is contrary to the values of the United States;

(2) the United States Government should not engage in the sale or transfer of facial recognition technology to any country that is using such technology for the suppression of human rights; and

(3) it is incumbent upon the intelligence community to develop clear policies and procedures that prevent the abuse of facial recognition technology.

(b) REPORT REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Director of Na-
tional Intelligence shall submit to the congressional intel-
ligence committees a report on the use of facial recognition
technology by the intelligence community. Such report
shall include each of the following:

(1) An analysis of the current use of facial rec-
ognition technology by the intelligence community.

(2) An analysis of the accuracy of facial rec-
ognition technology, including a discussion of the ap-
propriate threshold for use, and data disaggregated
by race, gender, ethnicity, and age.

(3) Whether the Government has adequate pro-
cedures in place to audit or test technology they pur-
chase to assess its accuracy, including on the basis
of race, gender, ethnicity, and age.

(4) The extent to which the intelligence commu-
nity has codified policies governing the use of facial
recognition technology that adequately prevent ad-
verse impacts on privacy, civil rights, and civil lib-
erties.

(5) An analysis of the ability of the intelligence
community to use facial recognition technology to
identify individuals in a way that respects constitu-
tional rights, civil rights, civil liberties, and privacy
of such individuals.
(6) Identification of risks and safeguards to uphold the constitutional rights, civil rights, civil liberties, and privacy of individuals, including for communities of color and religious minorities.

(7) Whether such technology is deployed in public areas or on photos of public areas in a manner that could raise First Amendment concerns.

(8) An identification of existing policies, procedures, or practices that permit the sharing of facial recognition data and technology with foreign governments or other non-United States Government entities.

(9) An identification of measures in place to protect data security.

(10) An identification of any redress procedures to address complaints in cases where the use of facial recognition resulted in harm to an individual.

(11) An analysis of existing transparency, oversight, and audits of the use of facial recognition to measure the efficacy of the technology on an ongoing basis, as measured against the cost and impact on individual rights.

(e) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.
(d) **FAcial Recognition Data Defined.**—In this section, the term “facial recognition data” means any unique attribute or feature of the face of an end user that is used by facial recognition technology to assign a unique, persistent identifier, or for the unique personal identification of a specific individual.