

108TH CONGRESS
1ST SESSION

S. _____

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN introduced the following bill; which was read twice and referred
to the Committee on _____

A BILL

To require a report on Federal Government use of commercial and other databases for national security, intelligence, and law enforcement purposes, 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 “Citizens’ Protection
5 in Federal Databases Act”.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

8 (1) Many Federal national security, law en-
9 forcement, and intelligence agencies are currently

1 accessing large databases, both public and private,
2 containing information that was not initially col-
3 lected for national security, law enforcement, or in-
4 telligence purposes.

5 (2) These databases contain personal and sen-
6 sitive information on millions of United States per-
7 sons.

8 (3) Some of these databases are subject to Fed-
9 eral privacy protections when in private sector con-
10 trol.

11 (4) Risks to personal privacy are heightened
12 when personal information from different sources,
13 including public records, is aggregated in a single
14 file and made accessible to thousands of national se-
15 curity, law enforcement, and intelligence personnel.

16 (5) It is unclear what standards, policies, proce-
17 dures, and guidelines govern the access to or use of
18 these public and private databases by the Federal
19 Government.

20 (6) It is unclear what Federal Government
21 agencies believe they legally can and cannot do with
22 the information once acquired.

23 (7) The Federal Government should be required
24 to adhere to clear civil liberties and privacy stand-
25 ards when accessing personal information.

1 (8) There is a need for clear accountability
2 standards with regard to the accessing or usage of
3 information contained in public and private data-
4 bases by Federal agencies.

5 (9) Without accountability, individuals and the
6 public have no way of knowing who is reading,
7 using, or disseminating personal information.

8 (10) The Federal Government should not access
9 personal information on United States persons with-
10 out some nexus to suspected counterintelligence, ter-
11 rorist, or other illegal activity.

12 **SEC. 3. LIMITATION ON USE OF FUNDS FOR PROCUREMENT**
13 **OR ACCESS OF COMMERCIAL DATABASES**
14 **PENDING REPORT ON USE OF INFORMATION.**

15 (a) LIMITATION.—Notwithstanding any other provi-
16 sion of law, commencing 60 days after the date of the en-
17 actment of this Act, no funds appropriated or otherwise
18 made available to the Department of Justice, the Depart-
19 ment of Defense, the Department of Homeland Security,
20 the Central Intelligence Agency, the Department of Treas-
21 ury, or the Federal Bureau of Investigation may be obli-
22 gated or expended by such department or agency on the
23 procurement of or access to any commercially available
24 database unless such head of such department or agency
25 submits to Congress the report required by subsection (b)

1 not later than 60 days after the date of the enactment
2 of this Act.

3 (b) REPORT.—(1) The Attorney General, the Sec-
4 retary of Defense, the Secretary of Homeland Security,
5 the Secretary of the Treasury, the Director of Central In-
6 telligence, and the Director of the Federal Bureau of In-
7 vestigation shall each prepare, submit to the appropriate
8 committees of Congress, and make available to the public
9 a report, in writing, containing a detailed description of
10 any use by the department or agency under the jurisdic-
11 tion of such official, or any national security, intelligence,
12 or law enforcement element under the jurisdiction of the
13 department or agency, of databases that were obtained
14 from or remain under the control of a non-Federal entity,
15 or that contain information that was acquired initially by
16 another department or agency of the Federal Government
17 for purposes other than national security, intelligence or
18 law enforcement, regardless of whether any compensation
19 was paid for such databases.

20 (2) Each report shall include—

21 (A) a list of all contracts, memoranda of under-
22 standing, or other agreements entered into by the
23 department or agency, or any other national secu-
24 rity, intelligence, or law enforcement element under
25 the jurisdiction of the department or agency for the

1 use of, access to, or analysis of databases that were
2 obtained from or remain under the control of a non-
3 Federal entity, or that contain information that was
4 acquired initially by another department or agency
5 of the Federal Government for purposes other than
6 national security, intelligence, or law enforcement;

7 (B) the duration and dollar amount of such
8 contracts;

9 (C) the types of data contained in the databases
10 referred to in subparagraph (A);

11 (D) the purposes for which such databases are
12 used, analyzed, or accessed;

13 (E) the extent to which such databases are
14 used, analyzed, or accessed;

15 (F) the extent to which information from such
16 databases is retained by the department or agency,
17 or any national security, intelligence, or law enforce-
18 ment element under the jurisdiction of the depart-
19 ment or agency, including how long the information
20 is retained and for what purpose;

21 (G) a thorough description, in unclassified
22 form, of any methodologies being used or developed
23 by the department or agency, or any intelligence or
24 law enforcement element under the jurisdiction of

1 the department or agency, to search, access, or ana-
2 lyze such databases;

3 (H) an assessment of the likely efficacy of such
4 methodologies in identifying or locating criminals,
5 terrorists, or terrorist groups, and in providing prac-
6 tically valuable predictive assessments of the plans,
7 intentions, or capabilities of criminals, terrorists, or
8 terrorist groups;

9 (I) a thorough discussion of the plans for the
10 use of such methodologies; and

11 (J) a thorough discussion of the policies, proce-
12 dures, guidelines, regulations, and laws, if any, that
13 have been or will be applied in the access, analysis,
14 or other use of the databases referred to in subpara-
15 graph (A), including—

16 (i) the personnel permitted to access, ana-
17 lyze, or otherwise use such databases;

18 (ii) standards governing the access, anal-
19 ysis, or use of such databases;

20 (iii) any standards used to ensure that the
21 personal information accessed, analyzed, or
22 used is the minimum necessary to accomplish
23 the intended legitimate Government purpose;

1 (iv) standards limiting the retention and
2 redisclosure of information obtained from such
3 databases;

4 (v) procedures ensuring that such data
5 meets standards of accuracy, relevance, com-
6 pleteness, and timeliness;

7 (vi) the auditing and security measures to
8 protect against unauthorized access, analysis,
9 use, or modification of data in such databases;

10 (vii) applicable mechanisms by which indi-
11 viduals may secure timely redress for any ad-
12 verse consequences wrongfully incurred due to
13 the access, analysis, or use of such databases;

14 (viii) mechanisms, if any, for the enforce-
15 ment and independent oversight of existing or
16 planned procedures, policies, or guidelines; and

17 (ix) an outline of enforcement mechanisms
18 for accountability to protect individuals and the
19 public against unlawful or illegitimate access or
20 use of databases.

21 **SEC. 4. GENERAL PROHIBITIONS.**

22 (a) IN GENERAL.—Notwithstanding any other provi-
23 sion of law, no department, agency, or other element of
24 the Federal Government, or officer or employee of the
25 Federal Government, may conduct a search or other anal-

1 ysis for national security, intelligence, or law enforcement
2 purposes of a database based solely on a hypothetical sce-
3 nario or hypothetical supposition of who may commit a
4 crime or pose a threat to national security.

5 (b) CONSTRUCTION.—The limitation in subsection
6 (a) shall not be construed to endorse or allow any other
7 activity that involves use or access of databases referred
8 to in section 3(b)(2)(A).

9 **SEC. 5. DEFINITIONS.**

10 In this Act:

11 (1) APPROPRIATE COMMITTEES OF CON-
12 GRESS.—The term “appropriate committees of Con-
13 gress” means—

14 (A) the Select Committee on Intelligence
15 and the Committee on the Judiciary of the Sen-
16 ate; and

17 (B) the Permanent Select Committee on
18 Intelligence and the Committee on the Judici-
19 ary of the House of Representatives.

20 (2) DATABASE.—The term “database” means
21 any collection or grouping of information about indi-
22 viduals that contains personally identifiable informa-
23 tion about individuals, such as individual’s names, or
24 identifying numbers, symbols, or other identifying
25 particulars associated with individuals, such as fin-

1 gerprints, voice prints, photographs, or other bio-
2 metrics. The term does not include telephone direc-
3 tories or information publicly available on the Inter-
4 net without fee.

5 (3) UNITED STATES PERSON.—The term
6 “United States person” has the meaning given that
7 term in section 101(i) of the Foreign Intelligence
8 Surveillance Act of 1978 (50 U.S.C. 1801(i)).