(2) otherwise inform the public of the activi-
ties of such officer, as appropriate and in a man-
ner consistent with the protection of class-
ified information and applicable law.

(h) Savings clause

Nothing in this section shall be construed to
limit or otherwise supplant any other authori-
ties or responsibilities provided by law to pri-
vacy officers or civil liberties officers.


AMENDMENTS

amendment, text of section read as follows: “It is the
sense of Congress that each executive department
or agency with law enforcement or antiterrorism func-
tions should designate a privacy and civil liberties offi-
cer.”

§ 2000ee–2. Privacy and data protection policies
and procedures

(a) Privacy Officer

Each agency shall have a Chief Privacy Officer
to assume primary responsibility for privacy and
data protection policy, including—

(1) assuring that the use of technologies sus-
tain, and do not erode, privacy protections rel-
ating to the use, collection, and disclosure of
information in an identifiable form;

(2) assuring that technologies used to col-
lect, use, store, and disclose information in
an identifiable form allow for continuous audit-
ing of compliance with stated privacy policies
and practices governing the collection, use
and distribution of information in the oper-
ation of the program;

(3) assuring that personal information con-
tained in Privacy Act systems of records is
handled in full compliance with fair informa-
tion practices as defined in the Privacy Act of
1974 (5 U.S.C. 552a);

(4) evaluating legislative and regulatory pro-
posals involving collection, use, and disclosure
of personal information by the Federal Gov-
ernment;

(5) conducting a privacy impact assessment
of proposed rules of the Department on the
privacy of information in an identifiable form,
including the type of personally identifiable
information collected and the number of peo-
ple affected;

(6) preparing a report to Congress on an an-
nual basis on activities of the Department
that affect privacy, including complaints of
privacy violations, implementation of section
552a of title 5, 11 other relevant matters;

(7) ensuring that the Department protects
information in an identifiable form and informa-
tion systems from unauthorized access,
use, disclosure, disruption, modification, or
destruction;

(8) training and educating employees on pri-
vacy and data protection policies to promote
awareness of and compliance with established
privacy and data protection policies; and

(9) ensuring compliance with the Depart-
ments established privacy and data protec-
tion policies.

(b) Establishing privacy and data protection pro-
cedures and policies

(1) In general

Within 12 months of December 8, 2004, each
agency shall establish and implement compre-
sensive privacy and data protection proce-
dures governing the agency’s collection, use,
sharing, disclosure, transfer, storage and secu-
ritv of information in an identifiable form rel-
lating to the agency employees and the public.
Such procedures shall be consistent with legal
and regulatory guidance, including OMB regu-
lations, the Privacy Act of 1974 [5 U.S.C. 552a],
and section 208 of the E-Government Act of
2002.

(c) Recording

Each agency shall prepare a written report of its
use of information in an identifiable form, along
with its privacy and data protection poli-
cies and procedures and record it with the In-
spector General of the agency to serve as a
benchmark for the agency. Each report shall be
signed by the agency privacy officer to verify
that the agency intends to comply with the pro-
cedures in the report. By signing the report the
privacy officer also verifies that the agency is
only using information in identifiable form as
detailed in the report.

(d) Inspector General review

The Inspector General of each agency shall pe-
riodically conduct a review of the agency’s im-
plementation of this section and shall report the
results of its review to the Committees on Ap-
propriations of the House of Representatives
and the Senate, the House Committee on Oversight
and Government Reform, and the Senate Com-
mittee on Homeland Security and Governmental
Affairs. The report required by this review may
be incorporated into a related report to Con-
gress otherwise required by law including, but
not limited to, section 3545 of title 44, the Fed-
eral Information Security Management Act of
2002. The Inspector General may contract with
an independent, third party organization to con-
duct the review.

(e) Report

(1) In general

Upon completion of a review, the Inspector
General of an agency shall submit to the head
of that agency a detailed report on the review,
including recommendations for improvements
or enhancements to management of informa-
tion in identifiable form, and the privacy and
data protection procedures of the agency.

(2) Internet availability

Each agency shall make each independent
third party review, and each report of the In-
spector General relating to that review avail-
able to the public.

(f) Definition

In this section, the definition of “identifiable
form” is consistent with Public Law 107–347, the

1 So in original.
2 So in original. Probably should be “Department’s”.
3 So in original. No par. (2) has been enacted.
E-Government Act of 2002, and means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.


REFERENCES IN TEXT

The Privacy Act of 1974, referred to in subsec. (a)(3) and (b)(1), is Pub. L. 93–579, Dec. 31, 1974, 88 Stat. 1896, which enacted section 552a of Title 5, Government Organization and Employees, and provisions set out as notes under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 and Tables.

Amendment note set out under section 552a of Title 5. For complete classification of this Act to the Code, see Short Title of 1974 Amendment note set out under section 552a of Title 5 and Tables.


Codification

Section was formerly set out as a note under section 552a of Title 5, Government Organization and Employees.

Amendments

2007—Subsec. (d). Pub. L. 110–161 added subsec. (d) and struck out former subsec. (d) which related to independent, third-party reviews.

§ 2000ee–3. Federal agency data mining reporting

(a) Short title

This section may be cited as the “FederalAgency Data Mining Reporting Act of 2007”.

(b) Definitions

In this section:

(1) Data mining

The term “data mining” means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where:

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

(2) Database

The term “database” does not include telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.

(c) Reports on data mining activities by Federal agencies

(1) Requirement for report

The head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made available to the public, except for an annex described in subparagraph (C).

(2) Content of report

Each report submitted under subparagraph (A) shall include, for each activity to use or develop data mining, the following information:

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

(C) A thorough description of the data sources that are being or will be used.

(D) An assessment of the efficacy or likely impact of the implementation of the data mining technology on the privacy and civil liberties of individuals, including a thorough discussion of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough discussion of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in

1 So in original. Probably should be “paragraph (3)’’.

2 So in original. Probably should be “paragraph (1)’’.