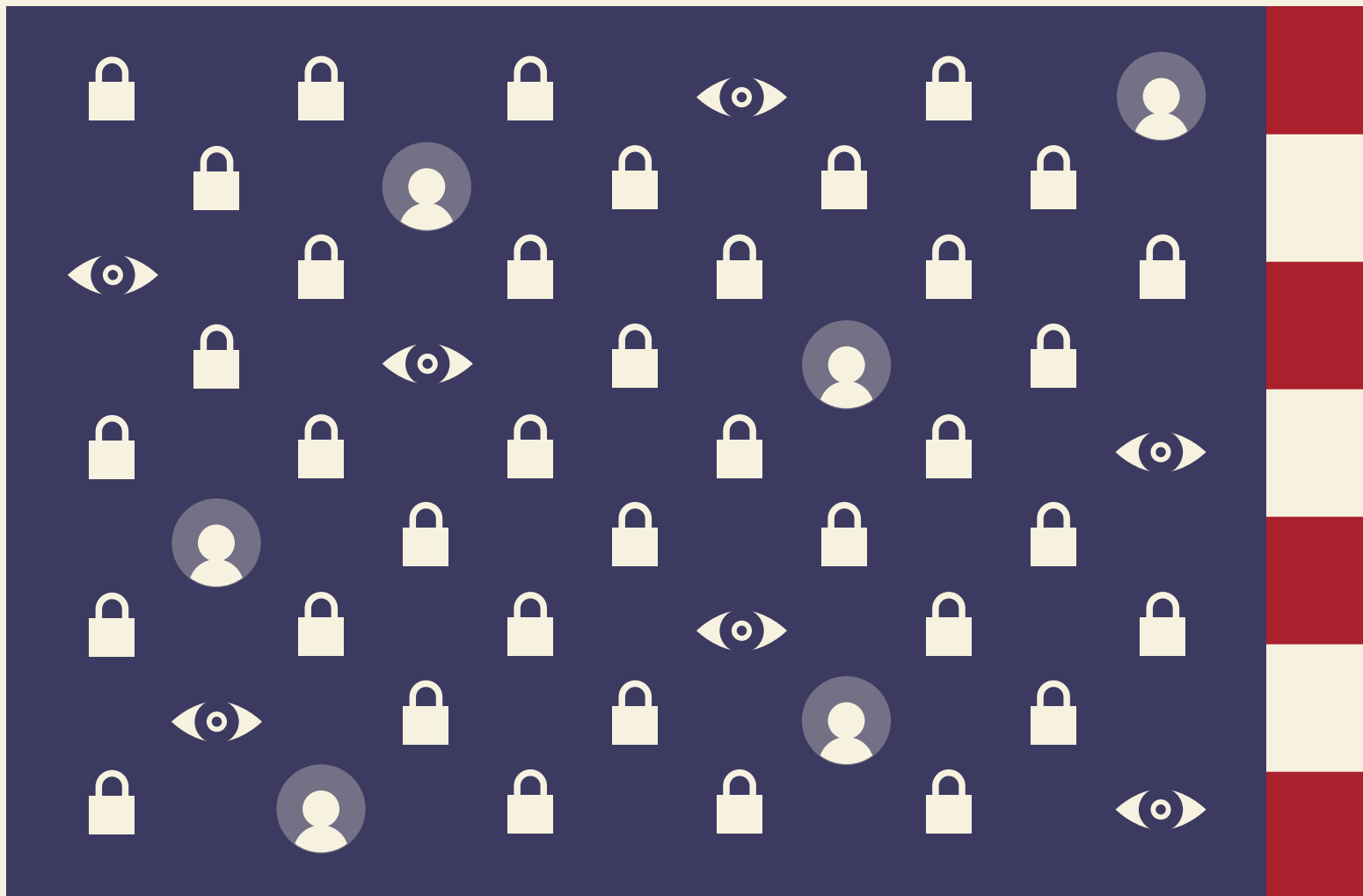


From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974

Appendix 1: Text of the Proposed United States Agency Fair Information Practices Act



From the Filing Cabinet to the Cloud: Updating the Privacy Act of 1974

5 U.S.C. § 552a

Appendix 1: Text of the Proposed United States Agency Fair Information Practices Act

PRIVACY ACT PROJECT

April 19, 2021
Version 2.01a

ROBERT GELLMAN
Privacy and Information Policy Consultant
419 Fifth Street SE
Washington, DC 20003

202-543-7923
bob@bobgellman.com
www.bobgellman.com

Appendix 1. Text of the Proposed United States Agency Fair Information Practices Act

Version 2.3

Sec. 1. Short Title.

This Act may be cited as the “United States Agency Fair Information Practices Act (USA FIPS Act)”.

Sec. 2. Findings and Purposes

(a) FINDINGS. – The Congress finds that –

(1) the right to privacy is a personal and fundamental right protected by the Constitution of the United States;

(2) the privacy of an individual is directly affected by the processing of personal information by Federal agencies;

(3) the increasing use of sophisticated information technology, data mining, artificial intelligence, and profiling of individuals and households greatly magnifies the harm to individual privacy that can occur from any unjustified, unnecessary, or careless processing of personal information;

(4) the opportunities for an individual to secure employment, insurance, and credit, to participate in social, political and economic marketplaces, and to achieve due process and other legal protections are endangered by any unjustified, unnecessary, or careless processing of personal information;

(5) in order to protect the privacy of individuals identified in information systems processed by Federal agencies, it is necessary and proper for the Congress to regulate the processing of personal information by the agencies;

(6) it is appropriate and important for Federal agencies to inform the public about the nature of agency personal information processing activities and for agencies to maintain accurate and current descriptions and records of those activities;

(7) reasonable implementation of the following principles of Fair Information Practices by Federal agencies will provide protections for individual privacy while allowing the Federal agencies to carry out their missions in an effective and efficient manner:

(A) the Principle of Collection Limitation provides that there should be limits to the collection of personally identifiable information, that the information should be collected by lawful and fair means, and that the information should be collected, where appropriate, with the knowledge or consent of the data subject;

(B) the Principle of Data Quality provides that personally identifiable information should be relevant to the purposes for which they are to be processed, and to the extent necessary for those purposes should be accurate, complete, and timely;

(C) the Principle of Purpose Specification provides that there must be limits to the processing of personally identifiable information and that the information should be processed only for the purposes specified at the time of collection and for compatible purposes;

(D) the Principle of Disclosure Limitation provides that personally identifiable information should not be disclosed, except as provided under the purpose specification principle, without the consent of the data subject or other legal authority;

1 (E) the Principle of Security provides that personally identifiable information should
2 be protected by reasonable security safeguards against risks including loss,
3 unauthorized access, destruction, use, modification, and disclosure;

4 (F) the Principle of Openness provides that the existence of record-keeping systems
5 containing personally identifiable information be publicly known, along with a
6 description of the record keeper, main purposes, uses, disclosures, policies, and
7 practices for processing the information;

8 (G) the Principle of Individual Participation provides that individuals should have a
9 right to see personally identifiable information about themselves and to seek
10 amendment or removal of information that is not timely, accurate, relevant, or
11 complete; and

12 (H) the Principle of Accountability provides that a record keeper should be
13 accountable for complying with fair information practices.
14

15 (b) PURPOSE. – The purposes of this Act are to provide safeguards for the personal privacy of
16 individuals by requiring Federal agencies, except as otherwise provided by law –

17 (1) to permit individuals to know how agencies process personally identifiable information;

18 (2) to restrict the use and disclosure of personally identifiable information to lawful, defined,
19 and disclosed purposes;

20 (3) to permit data subjects to gain access to personally identifiable information pertaining to
21 themselves in Federal agency records, to have a copy of the records, and to ask for amendment to the
22 records;

23 (4) to process any record in a manner that assures that –

24 (A) the processing is for a necessary and lawful purpose;

25 (B) the personally identifiable information in the record is current and accurate for its
26 intended use; and

27 (C) the processing provides adequate safeguards to prevent misuse of the information;

28 (5) to be subject to civil suit for any damages which occur as a result of willful or intentional
29 action that violates any individual's rights under this Act; and

30 (6) to allow any person who believes that a Federal agency is not complying with this Act to
31 ask the agency to bring its conduct into compliance.
32

33 **Sec. 3. Definitions.**

34 In this Act:

35
36
37 • (1) INDIVIDUAL. –The term “individual” means a living individual and includes an
38 individual acting as a sole proprietor.

39
40 (2) DATA SUBJECT. –The term “data subject” means the individual who is the
41 principal subject of a record.
42

43 (3) PERSONALLY IDENTIFIABLE INFORMATION. – The term "personally identifiable
44 information" means information about an identified or identifiable individual, including information
45 about location, housing, education, finances, health, employment, criminal history, military service,
46 taxation, agency program participation, Internet usage history, or any other personal activity or
47 characteristic, and that contains any of the following data:

48 (A) a name;

1 (B) a home address, post office box, private mail box, or other physical or postal address;
2 (C) an e-mail address;
3 (D) a telephone number or the letters and numbers of a vehicle license plate;
4 (E) a Social Security Number; passport number; credit or debit card number; account, license,
5 or employee number; or other identifying number assigned to an individual;
6 (F) date of birth;
7 (G) an Internet Protocol address or any comparable successor address;
8 (H) any other data that permits the physical or online contacting of a specific individual;
9 (I) a photograph, fingerprint, genetic, or other biometric identifier;
10 (J) information that identifies an individual's electronic device, including an international
11 mobile equipment identity number, media access control address, contactless chip identifier, or any
12 information that an agency Web site or online service collects online through a computer or from the
13 individual, individual's cell phone, or other electronic device; or
14 (K) other information concerning an individual processed in combination with an identifier
15 described in subparagraphs (A) through (J).
16

17 (4) AGENCY ACTIVITY AFFECTING PRIVACY. –The term “agency activity affecting
18 privacy” means any agency function, program, or conduct that involves the processing of a record
19 about an individual.
20

21 (5) RECORD. – The term “record” means any personally identifiable information
22 processed by or for an agency as part of an agency activity affecting privacy.
23

24 (6) USE. –The term “use” means, with respect to a record, the employment, application,
25 utilization, examination, sharing, or transfer of the record within the agency that processes the record.
26

27 (7) DISCLOSURE. –The term “disclosure” means, with respect to a record, the release,
28 transfer, provision of access to, or divulging in any other manner of the record outside the agency that
29 processes the record.
30

31 (8) PROCESSING. –The term “processing” or “processed” means, an activity with respect to a
32 record, including the creation, collection, use, disclosure, maintenance, storage, examination, analysis,
33 encryption, decryption, deidentification, reidentification, erasure, or destruction of the record.
34

35 (9) AGENCY DESIGNATED DISCLOSURE. – The term “agency designated disclosure”
36 means a disclosure by an agency of a record from an agency activity affecting privacy that is –
37 (A) required or specifically authorized by Federal statute or treaty;
38 (B) appropriate to carry out the function of the agency activity affecting privacy from which
39 the disclosure is made and for which the record was collected; or
40 (C) in support of another specified Federal activity or other specified activity
41 for which the agency can appropriately disclose a record and the disclosure is not inconsistent
42 with the purpose for which the record was collected.
43

44 (10) AGENCY. –The term “agency” means an agency as defined in section 552(f) of title 5,
45 United States Code, and the Government Accountability Office, the Library of Congress, the
46 Administrative Office of the United States Courts, the Government Printing Office, and the
47 Smithsonian Institution.

1
2 (11) CLASSIFIED INFORMATION. – The term “classified information” means any
3 information (1) specifically authorized under criteria established by an Executive order to be kept
4 secret in the interest of national defense or foreign policy; and (2) in fact properly classified pursuant
5 to the Executive order.
6

7 (12) MATCHING PROGRAM. – The term “matching program” –
8 (A) means any automated comparison or other activity that involves the disclosure of –
9 (i) records processed in two or more two agency activities affecting privacy or from an agency
10 activity affecting privacy with non-Federal agency records for the purpose of –
11 (I) establishing or verifying the eligibility of, or continuing compliance with statutory and
12 regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers
13 of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or
14 (II) recouping payments or delinquent debts under Federal benefit programs, or
15 (ii) Federal personnel or payroll records from two or more agency activities affecting privacy
16 or from an agency activity affecting privacy with non-Federal agency records; but
17 (B) does not include –
18 (i) matches performed to support any research, statistical, or other activity, if the results of
19 the matching are not intended to be used and are not used to make decisions concerning the rights,
20 benefits, privileges, or status of specific individuals or to take any adverse financial, personnel,
21 disciplinary, or other adverse action against Federal personnel;
22 (ii) matches performed, by an agency (or component thereof) which performs as its principal
23 function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a
24 specific criminal or civil law enforcement investigation of a named person or persons for the purpose
25 of gathering evidence against the person or persons;
26 (iii) matches of tax information pursuant to the Internal Revenue Code of 1986 or for the
27 purpose of intercepting a tax refund due an individual under authority granted by statute;
28 (iv) matches performed for foreign counterintelligence purposes or to produce background
29 checks for security clearances of Federal personnel or Federal contractor personnel; or
30 (v) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act
31 (42 U.S.C. 402(x)(3), 1382(e)(1)).
32
33

34 (13) RECIPIENT AGENCY. – The term “recipient agency” means any agency, or contractor
35 thereof, receiving records processed as part of an agency activity affecting privacy of a source agency
36 for use in a matching program.
37

38 (14) NON-FEDERAL AGENCY. – The term “non-Federal agency” means any State or local
39 government, or agency thereof, that receives records processed as part of an agency activity affecting
40 privacy from a source agency for use in a matching program.
41

42 (15) SOURCE AGENCY. – The term “source agency” means any (A) agency that discloses
43 records processed as part of an agency activity affecting privacy to be used in a matching program, or
44 (B) State or local government, or agency thereof, that discloses records to be used in a matching
45 program.
46

1 (16) FEDERAL BENEFIT PROGRAM. – The term “Federal benefit program” means any
2 program administered or funded by the Federal Government, or by any agent or State on behalf of the
3 Federal Government, providing cash, payments, grants, loans, loan guarantees, or other forms of in-
4 kind assistance to individuals.

5
6 (17) FEDERAL PERSONNEL. – The term personnel” means officers and employees of the
7 Government of the United States, members of the uniformed services (including members of the
8 Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits
9 under any retirement program of the Government of the United States (including survivor benefits).

10
11 **Sec. 4. General Processing Requirements.**

12
13 (a) RELEVANT AND NECESSARY. – Each agency shall process only personally identifiable
14 information that is relevant and necessary to accomplish a purpose of the agency required to be
15 accomplished by law or executive order of the President.

16
17 (b) DIRECT COLLECTION. – Each agency shall collect personally identifiable information to
18 the extent practicable directly from the data subject when the personally identifiable information may
19 result in adverse determinations about the data subject’s rights, benefits, privileges, or status under
20 Federal programs.

21
22 (c) NOTICE. – Each agency shall, in writing or otherwise and in understandable language,
23 inform each data subject whom it asks to supply personally identifiable information, at the time of
24 collection and in a manner that allows the data subject to obtain or retain a copy, of the following:

25 (1) the authority for the collection;

26 (2) the principal purpose or purposes for which the personally identifiable information will be
27 used;

28 (3) the agency designated disclosures that may be made of the personally identifiable
29 information; and

30 (4) whether the data subject is required by law to supply the personally identifiable
31 information and the consequences of not providing all or any part of the personally identifiable
32 information.

33
34 (d) DETERMINATIONS. – Each agency shall process records used by the agency in making
35 any determination about a data subject with sufficient accuracy, relevance, timeliness, and
36 completeness as is reasonably necessary to assure fairness to the data subject in the determination.

37
38 (e) DISCLOSURE. – Prior to disclosing any personally identifiable information to any person
39 other than an agency, unless the dissemination is made pursuant to section 552, title 5, United States
40 Code, each agency shall make reasonable efforts to assure that the personally identifiable information
41 is accurate, complete, timely, and relevant for agency purposes.

42
43 (f) FIRST AMENDMENT. – No agency shall process a record describing how any individual
44 exercises rights guaranteed by the First Amendment unless expressly authorized by statute, or by the
45 individual, or unless pertinent to and within the scope of an authorized law enforcement activity.

1 (g) LEGAL PROCESS. – Each agency shall make reasonable efforts to serve notice on a data
2 subject when any personally identifiable information about the data subject is made available to any
3 person under compulsory legal process when the process becomes a matter of public record.
4

5 (h) SAFEGUARDS. – Each agency shall, consistent with the requirements in subchapter II of
6 chapter 35 of title 44, United States Code, establish appropriate administrative, technical, and physical
7 safeguards to ensure the security and confidentiality of records and to protect against any anticipated
8 threats or hazards to their security or integrity that could result in substantial harm, embarrassment,
9 inconvenience, or unfairness to any data subject.
10

11 **Sec. 5. Agency Activity Affecting Privacy.**
12

13 (a) SCOPE. – Each agency shall determine the scope of each agency activity affecting privacy
14 so as to reflect accurately its processing of records and to do so in a manner that supports public
15 understanding of agency operations.
16

17 (b) GUIDANCE. –The Director of the Office of Management and Budget shall issue guidance
18 to agencies about determining the scope of an agency activity affecting privacy. The guidance shall
19 advise agencies how to address these goals to the extent practicable:

- 20 (1) the goal of grouping activities with similar or related purposes within the same agency
21 activity affecting privacy;
- 22 (2) the goal of grouping activities based on similar authority within the same agency activity
23 affecting privacy;
- 24 (3) the goal of keeping records eligible for exemptions separate from non-exempt activities;
25 and
- 26 (4) the goal of defining agency activities affecting privacy so that agency designated disclosures
27 do not apply to records unnecessarily.
28

29 (c) DESCRIPTION. – For each agency activity affecting privacy, an agency shall prepare and
30 maintain a description that shall include –

- 31 (1) the name of the activity, the scope of the activity, each principal substantive purpose that
32 the activity supports, and the authority for the activity, including any related information collection
33 requests approved under the Paperwork Reduction Act;
- 34 (2) the name of the agency component primarily responsible for the activity, the principal
35 postal, electronic mail, and website addresses of that component, and the name of other agency
36 components that significantly participate in the activity;
- 37 (3) the categories of data subjects about whom records are processed as part of the activity;
- 38 (4) the categories of records processed in the activity;
- 39 (5) the principal information technologies employed, including any novel or innovative
40 applications of technology; any automated decision making; any processing of records using artificial
41 intelligence; any algorithmic development, analysis, or application; or any similar activities with the
42 potential to affect the rights or interests of data subjects;
- 43 (6) each agency designated disclosure applicable to records processed as part of the activity,
44 including a good faith effort to list agency designated disclosures in the approximate order in which
45 they are likely to be used, with the most used disclosure listed first;
- 46 (7) the categories of sources of records in the activity, including any commercial,
47 governmental, or other sources that the agency routinely reviews, consults, or otherwise uses to carry
48 out the activity;

1 (8) the policies and practices of the agency regarding storage, retrievability, access controls,
2 retention, and disposal of records in the activity, including the name and location of records disposal
3 schedules covering any of the records;

4 (9) the location of the agency website and of the agency's rules where an individual can learn
5 how to exercise rights available under this Act;

6 (10) whether the activity is likely to include any records subject to an exemption in section 12
7 of this Act; describing the reasons exempt records may be included; and describing how the
8 exemption affects any rights available under this Act;

9 (11) the date the description was most recently published or amended; and

10 (12) a reference where the agency publishes any personally identifiable information processing
11 diagram for the activity and any publicly available privacy impact assessment conducted by the agency
12 relevant to the activity.

13
14 (d) PUBLICATION. – An agency shall publish the following notices, including the description
15 of each agency activity affecting privacy prepared as provided in subsection (c) –

16 (1) For the initial publication of a description of an agency activity affecting privacy, the
17 agency shall publish a complete notice in the Federal Register as provided in section 553(b) and (c) of
18 title 5, United States Code.

19 (2) For any material change in an agency activity affecting privacy, including a new or
20 modified purpose or agency designated disclosure, the agency shall –

21 (A) publish a notice of the proposed change in the activity in the Federal Register as provided
22 in section 553(b) and (c) of title 5, United States Code;

23 (B) provide, either as part of the Federal Register notice or on the agency's website, the full
24 text of the description of the activity clearly identifying the proposed change; and

25 (C) if the agency only provides the full text of the description on its website, make the full text
26 available on or before the date when the public comment period begins.

27 (3) For a non-material change in an agency activity affecting privacy or in an agency
28 designated disclosure, the agency shall publish a notice describing the change in the Federal Register
29 and provide on its website the full text of the revised description of the agency activity affecting
30 privacy that clearly identifies the proposed change.

31
32 (e) FULL TEXT REQUIRED. – In any published description or proposed modification of an
33 agency activity affecting privacy or agency designated disclosure, an agency shall include the full text
34 of each agency activity affecting privacy or each agency designated disclosure and not by reference to
35 another document.

36
37 (f) JOINT AGENCY ACTIVITIES AFFECTING PRIVACY. – The Director of the Office of
38 Management and Budget shall issue guidance covering any agency activity affecting privacy operated
39 by one agency on behalf of one or more other agencies or for which more than one agency has a
40 responsibility. The guidelines shall prescribe how the requirements of this Act shall be allocated
41 among the agencies involved and how the duties imposed by this Act shall be carried out.

42 43 **Sec. 6. Allowable Uses and Disclosures.**

44
45 (a) USE. – An agency may allow those officers and employees of the agency who have a need
46 for a record from an agency activity affecting privacy to use the record in the performance of their
47 duties. Nothing in this subsection expands or reduces the ability of an agency to –

48 (1) use or withhold from use a record as otherwise provided by statute; or

1 (2) withhold a record used for one agency function from another agency function.
2

3 (b) DISCLOSURE. – No agency shall disclose any record by any means of communication to
4 any person, or to another agency, except pursuant to a written request by, or with the prior written
5 consent of, the data subject, unless disclosure of the record is otherwise allowed under this section.
6

7 (c) AGENCY DESIGNATED DISCLOSURE. – An agency may disclose a record if the
8 disclosure is for an agency designated disclosure adopted by the agency pursuant to section 5.
9

10 (d) ALLOWABLE DISCLOSURES. – An agency may disclose a record if the disclosure is the
11 following:

12 (1) REQUIRED BY FOIA. – The disclosure is required under section 552 of title 5, United
13 States Code.

14 (2) STATISTICAL AGENCY DISCLOSURE. – The disclosure is to a statistical agency or unit
15 for statistical purposes, as those terms are defined in section 3561 of title 44, United States Code, and
16 subject to the provisions, including the limits on use and disclosure, of section 3572 of title 44, United
17 States Code.

18 (3) ARCHIVES DISCLOSURE. – The disclosure is to the National Archives and Records
19 Administration –

20 (A) for a record that has sufficient historical or other value to warrant its continued
21 preservation by the United States Government;

22 (B) for evaluation by the Archivist of the United States or the designee of the Archivist to
23 determine whether the record has that value; or

24 (C) pursuant to a records management inspection as provided in chapter 29 of title 44, United
25 States Code.

26 (4) REQUEST FROM LAW ENFORCEMENT AGENCY. – The disclosure is to another
27 agency or to an instrumentality of any governmental jurisdiction within or under the control of the
28 United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if
29 the head of the agency or instrumentality made a written request to the agency that processes the
30 record specifying the particular portion desired and the law enforcement activity for which the record
31 is sought.

32 (5) CIVIL OR CRIMINAL LAW ENFORCEMENT. – The disclosure is to the appropriate
33 Federal, State, local, tribal, or foreign agency responsible for investigating, prosecuting, enforcing, or
34 implementing a statute, rule, regulation, or order, if the record is relevant to a violation or potential
35 violation of civil or criminal law or regulation within the jurisdiction of the receiving agency.

36 (6) HEALTH OR SAFETY. – The disclosure is to a person if –

37 (A) the agency believes in good faith that –

38 (i) the disclosure is necessary to prevent or lessen a serious and imminent threat to the health
39 or safety of any individual or the public and

40 (ii) the person is reasonably able to prevent or lessen the threat; and

41 (B) the agency making a disclosure under this paragraph sends a notice of the disclosure to the
42 data subject's last known physical or electronic mail address, unless the Chief Privacy Officer
43 determines that sending a notice would be inappropriate and documents the reason for the
44 determination in writing.

45 (7) CONGRESS. – The disclosure is to either House of Congress, or, to the extent of matter
46 within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or
47 subcommittee of any the joint committee.

1 (8) WRITTEN INQUIRY TO MEMBER OF CONGRESS. –The disclosure is to a Member of
2 Congress in response to a written inquiry by the Member of Congress after the Member of Congress
3 receives a written request from the data subject pertaining to or concerning a matter contained in the
4 record.

5 (9) GOVERNMENT ACCOUNTABILITY OFFICE. – The disclosure is to the Comptroller
6 General, or any authorized representative of the Comptroller General, in the course of the
7 performance of the duties of the Government Accountability Office.

8 (10) CONTRACTORS, GRANTEEES, OTHERS. – The disclosure is to a contractor, grantee,
9 consultant, or volunteer performing or working on a contract, grant, cooperative agreement, or
10 otherwise for the agency and who has a need for the record in the performance of their duties for the
11 agency. When required, the recipient shall comply with section 14.

12 (11) COURTS AND LITIGATION. – The disclosure –

13 (A) is pursuant to the order of a court of competent jurisdiction;

14 (B) occurs in a filing made in a court of competent jurisdiction pursuant to the rules of that
15 court;

16 (C) is to a party in litigation with the agency, is authorized by the rules or order of the court or
17 adjudicative body conducting the proceeding before which the litigation is pending, and a rule, order,
18 or a signed written agreement, limits use of the disclosed record to the purpose of conducting the
19 litigation; or

20 (D)(i) is to a party, or potential party, to litigation with the agency, or to the party's
21 authorized representative, or to an independent mediator, in connection with settlement
22 discussions; and

23 (ii) the disclosure of the record is limited to the purposes of the settlement negotiations by
24 (I) a rule or order of the court or adjudicative body conducting the proceeding, or (II) a written
25 agreement signed by the parties.

26 (12) DATA BREACH RESPONSE. – The disclosure is –

27 (A) for the purpose of responding to a suspected or confirmed data breach that involves a risk
28 of harm to an individual or a data system;

29 (B) approved by –

30 (i) the head of the agency;

31 (ii) the Chief Privacy Officer of the agency;

32 (iii) a senior agency official designated under a written agency data breach response plan; or

33 (iv) the Federal Chief Privacy Officer;

34 (C) of records from an agency activity affecting privacy that an agency official supervising the
35 data breach response determines are (i) likely to be relevant to the purpose of this paragraph; and (ii)
36 made to an agency, entity, or other person for which the official approving the disclosure has reason to
37 believe may be able to assist in identifying the existence or scope of a data breach or in responding to
38 the data breach either by providing a remedy for an individual who may have been affected by the data
39 breach or by assisting with protection of a data system; and

40 (D) pursuant to a contract or agreement limiting the use of all data disclosed to the purpose of
41 the disclosure and requiring either the prompt return or destruction of all data disclosed when the
42 agency determines that the purposes of the disclosure are fulfilled.

43 (13) FEDERAL PERSONNEL AND OTHER DECISIONS. – The disclosure is to those officials
44 and employees of a Federal agency or Federal entity that require personally identifiable information
45 relevant to a decision about (i) the hiring, appointment, or retention of an employee; (ii) the issuance,
46 renewal, suspension, or revocation of a security clearance; (iii) a security or suitability investigation;
47 (iv) the awarding of a contract or grant; or (v) the issuance of a grant or benefit.
48

1 (e) MINIMIZE ALLOWABLE DISCLOSURES. – When disclosing a record pursuant to an
2 allowable disclosure in subsection (d), an agency shall make a good faith effort to disclose the
3 minimum amount of personally identifiable information that will accomplish the purpose of the
4 disclosure.

5
6 (f) PROCEDURAL REQUIREMENTS FOR AGENCY DESIGNATED DISCLOSURES.

7 (1) CPO APPROVAL. All agency designated disclosures must be approved by the agency’s
8 Chief Privacy Officer pursuant to section 9(b)(6);

9 (2) DESCRIPTION. – When establishing an agency designated disclosure, the agency shall to
10 the extent practicable identify as part of the description of the disclosure –

11 (A) why the disclosure qualifies under one or more of the subparagraphs (A), (B), and (C) in
12 the definition of “agency designated disclosure” in section 3(9);

13 (B) the class of recipients of personally identifiable information;

14 (C) the types of personally identifiable information that may be disclosed;

15 (D) the purpose of and authority for the disclosure, including a good faith effort to specify
16 each statute or treaty that requires or specifically authorizes disclosure of personally identifiable
17 information;

18 (E) the position description or function of those agency officers and employees who may
19 authorize a disclosure as an agency designated disclosure.

20 (3) MINIMIZING DISCLOSURE. –

21 (A) When establishing an agency designated disclosure, an agency shall as part of the
22 description of the disclosure and to the extent practicable, limit each agency designated disclosure to
23 those records and to those portions of records processed in an agency activity affecting privacy that
24 fulfill the purpose for which the agency designated disclosure was established;

25 (B) When disclosing a record pursuant to an agency designated disclosure, an agency shall to
26 the extent practicable disclose the minimum amount of personally identifiable information that will
27 accomplish the purpose of the disclosure.

28 (4) PUBLIC DISCLOSURE. – If an agency designated disclosure authorizes the public
29 disclosure of personally identifiable information, the agency shall establish a procedure that requires
30 the approval of the Chief Privacy Officer prior to the disclosure. This paragraph does not apply to
31 disclosures required by section 552 of title 5, United States Code, or to other public disclosures
32 required by law.

33
34 (g) OMB GUIDANCE. –

35 (1) ALTERNATIVE TO CONSENT. – The Director of the Office of Management and Budget
36 shall issue guidance discouraging agencies from establishing agency designated disclosures principally
37 as an alternative to obtaining consent of the data subject.

38 (2) MODEL NOTICES. – The Director of the Office of Management and Budget may prepare
39 and publish for the use of agencies model notices of agency designated disclosures that are likely to be
40 relevant to many agencies. Any agency that proposes to adopt an agency designated disclosure
41 addressing disclosures covered by a model notice published in accordance with this paragraph that
42 differs from the model notice by allowing for broader or additional disclosures shall explain its reasons
43 when it publishes the agency designated disclosure for public comment.

44
45 (h) LIMITS. – Except as otherwise provided by law, nothing in this Act requires an agency to
46 disclose a record to anyone other than the data subject or to a parent, guardian, or other person
47 identified in section 16(d).

1 **Sec. 7. Access to and Amendment of Records.**

2
3 (a) ACCESS. – (1) An agency shall upon request by a data subject regarding a record
4 processed as part of an agency activity affecting privacy permit the data subject and any person chosen
5 by the data subject to review the record and to have a copy of any or all of the record in any form or
6 format requested by the data subject if the record is readily reproducible by the agency in that form or
7 format.

8 (2) An agency shall acknowledge in writing or by electronic mail receipt of a request under
9 this subsection within ten days of receipt and shall provide the requested record within 30 days. If the
10 request is denied in whole or in part, the agency shall inform the data subject of the denial, the reason
11 for the denial, and the procedures established by the agency for appealing the denial to the head of the
12 agency or designee.

13 (3) If after an appeal of a denial of a request for review or copy of a record, the agency refuses
14 to provide the review or copy, the agency shall inform the data subject of the reasons for the denial
15 and of the procedures for judicial review.

16 (4) For any request under this subsection and section 8(b)(2), an agency shall also provide to a
17 data subject any requested information that would be available to the data subject under section 552
18 of title 5, United States Code.

19
20 (b) AMENDMENT. – (1) An agency shall upon request by a data subject permit the data
21 subject to request amendment of a record processed as part of an agency activity affecting privacy
22 pertaining to the data subject that the data subject believes is not accurate, relevant, timely, or
23 complete.

24 (2) An agency shall acknowledge in writing or by electronic mail receipt of a request under
25 this subsection within ten days of receipt and shall within 30 days of the receipt of the request, either
26 –

27 (A) make any amendment that the data subject requested, and promptly inform the data
28 subject of the amendment; or

29 (B) inform the data subject of its refusal to make the requested amendment, the reason for the
30 refusal, the procedures established by the agency for appealing the refusal to the head of the agency or
31 designee.

32 (3) An agency shall within 30 days of the receipt of an appeal by the data subject of a denial of
33 a request for amendment either –

34 (A) make any amendment that the data subject requested, and promptly inform the data
35 subject of the amendment; or

36 (B) inform the data subject of –

37 (i) the right to file with the agency a concise statement setting forth the reasons for the data
38 subject's disagreement with the refusal of the agency; and

39 (ii) the right to judicial review of the denial.

40 (4) In any future disclosure of a record or portion of a record about which a data subject filed a
41 statement of disagreement, the agency shall clearly identify any disputed information and, unless the
42 data subject objects in writing, provide a copy of the data subject's statement of disagreement and, if
43 the agency chooses, a statement describing the agency's reasons for not making the amendment
44 requested.

45
46 (c) EXTENSION. – The Chief Privacy Officer may extend the deadlines for responding to a
47 request under this section for (1) review or a copy of a record, or (2) for an amendment, in each case
48 by no more than 30 days, by notifying the data subject making a request in writing or by electronic
49 mail.

1
2 **Sec. 8. Disclosure History**
3

4 (a) ACCURATE DISCLOSURE HISTORY REQUIRED. – Each agency, with respect to each
5 agency activity affecting privacy, shall except for uses made under section 6(a) and disclosures made
6 under section 6(d)(1), keep or maintain the ability to create upon request an accurate history of –

7 (1) the date, nature, and purpose of each disclosure of a record to any person or to another
8 agency made pursuant to an agency designated disclosure; and

9 (2) the name and address of the person or agency to whom the disclosure is made;

10 (b) RETENTION, AVAILABILITY, AND NOTICE OF DISCLOSURE HISTORY. – Each
11 agency shall –

12 (1) keep or maintain the ability to create upon request a disclosure history for at least five
13 years after the disclosure or for the life of the record, whichever is longer;

14 (2) except for disclosures made under section 6(d)(2), (3), (4) and (5), make the disclosure
15 history available to the data subject upon a request made pursuant to the access procedure described
16 in section 7(a); and

17 (3) inform any person or other agency about any amendment or statement of disagreement
18 made in accordance with section 7 of any record previously disclosed to the person or agency if a
19 disclosure history is available, if the data subject who requested the amendment or submitted a
20 statement of disagreement asks that the amendment or statement be disclosed.

21
22 **Sec. 9. Chief Privacy Officer.**
23

24 (a) CHIEF PRIVACY OFFICER. – The head of each agency shall, promptly after the effective
25 date of this Act, designate a Chief Privacy Officer to carry out the functions assigned under this Act
26 and other related functions. If another statute established a privacy officer or similar officer for the
27 agency, the head of the agency may designate that officer to carry out the functions assigned under
28 this Act.

29
30 (b) DUTIES. – The Chief Privacy Officer for an agency shall –

31 (1) have agency-wide responsibility for privacy and for compliance with fair information
32 practices;

33 (2) have agency-wide responsibility for overseeing agency compliance with Federal laws,
34 regulations, and policies relating to privacy, including primary responsibility for implementation of
35 this Act;

36 (3) participate in identifying and addressing privacy risks throughout the agency;

37 (4) have responsibility for agency privacy impact assessments as provided in section 11;

38 (5) have a central role in the agency’s development and evaluation of legislative, regulatory,
39 and other policy proposals relating to or affecting the privacy of personally identifiable information;
40 and

41 (6) approve the publication of the description of each agency activity affecting privacy,
42 including each agency designated disclosure, prior to publication for comment and before the
43 description and the agency designated disclosure becomes final.

44
45 (c) NOTICES. –The Chief Privacy Officer shall, to the extent practicable, standardize
46 elements and terminology of notices of agency activities affecting privacy, including agency designated
47 disclosures.
48

1 (d) Personally Identifiable Information Processing Diagram. – The Chief Privacy Officer shall,
2 to the extent practicable, maintain on the agency privacy website for each major agency activity
3 affecting privacy a current personally identifiable information processing diagram or equivalent
4 document that visually depicts the collection, use, and disclosure of personal information and that
5 shows the principal sources of information, the principal internal users of the personal information,
6 the principal purposes for which the agency collects and discloses personal information, and the
7 recipients of the disclosures.

8
9 (e) REPORT. –When the Chief Privacy Officer of an agency determines that a threat or
10 vulnerability is creating or is likely to create a significant disruption to the privacy responsibilities of
11 the agency, a serious unresolved privacy or security risk to the agency, or an inappropriate or
12 avoidable serious privacy or security risk to data subjects, the Chief Privacy Officer may –

- 13 (1) consult with the Chief Information Officer of the agency; and
14 (2) report from time to time directly to the head of the agency.

15
16 (f) GUIDANCE. –The Director of the Office of Management and Budget may issue guidance
17 on the activities and functions of a Chief Privacy Officer, including guidance on the preparation and
18 format of personally identifiable information processing diagrams prepared under subsection (d).

19
20 **Sec. 10. Federal Chief Privacy Officer at the Office of Management and Budget.**

21
22 (a) FEDERAL CHIEF PRIVACY OFFICER. –The Director of the Office of Management and
23 Budget shall, promptly after the effective date of this Act, establish an Office of the Federal Chief
24 Privacy Officer as part of the Office of Information and Regulatory Affairs. A Federal Chief Privacy
25 Officer shall head the Office of the Federal Chief Privacy Officer.

26
27 (b) DUTIES. –The Office of the Federal Chief Privacy Officer shall –
28 (1) have responsibility for preparing Office of Management Budget guidance under this Act;
29 (2) provide notice and opportunity for public comment for the guidance;
30 (3) assist and direct agencies with the transition from compliance with the Privacy Act of 1974
31 to compliance with this Act;
32 (4) oversee agency compliance with this Act and provide continuing assistance to agencies
33 with the implementation of this Act; and
34 (5) have responsibility for advising the Director on all privacy matters.

35
36 **Sec. 11. Privacy Impact Assessment Process.**

37
38 (a) PURPOSE. – The purposes of the privacy impact assessment process are –
39 (1) to inform agency decisions for the life cycle of agency activities affecting privacy, including
40 planning, design, implementation, and conduct, in a manner consistent with other Federal
41 information resources management policies, principles, standards, and guidelines;
42 (2) to identify significant risks to the agency and significant consequences for the privacy of
43 data subjects from the conduct of agency activities affecting privacy;
44 (3) to seek and implement ways to minimize significant risks and consequences prior to
45 establishing or modifying an agency activity affecting privacy while providing for the efficient and
46 effective conduct of agency responsibilities;
47 (4) to provide that agency processing of personal information minimizes the processing of
48 personally identifiable information, maximizes fairness, includes appropriate due process protections,
49 and generally complies with fair information practices;

1 (5) to provide to the extent practicable an opportunity for public comment in the planning
2 and design of an agency activity affecting privacy;

3 (6) to complete the process, to the extent practicable, before the agency makes final decisions
4 about the design of an agency activity affecting privacy; and

5 (7) to document the conduct of the process with a written report.
6

7 (b) PROCESS. –

8 (1) Each agency shall conduct either a thorough or a limited privacy impact assessment
9 process for new or significantly modified agency activities affecting privacy and for new or
10 significantly revised matching programs.

11 (2) In determining whether to conduct a thorough or a limited privacy impact assessment
12 process, an agency shall consider using a thorough assessment when agency activities affecting privacy
13 are reasonably likely to have one or more of these characteristics:

14 (A) affect a large number of data subjects;

15 (B) involve determinations of eligibility for rights, benefits, privileges, or status;

16 (C) employ or propose to employ any novel or innovative applications of technology;

17 (D) present significant risks to the agency or significant consequences for the privacy
18 of data subjects;

19 (E) involve the routine collection of records from sources outside the Federal
20 government or the routine disclosure of records outside the Federal government; or

21 (F) result in significant new mergers of previously separate government databases.

22 (3) The Director of the Office of Management and Budget shall issue guidance to help
23 agencies –

24 (A) decide whether to conduct either a thorough or a limited privacy impact assessment
25 process;

26 (B) establish priorities for conducting privacy impact assessment processes;

27 (C) address privacy –

28 (i) as part of the information and information system life cycles;

29 (ii) in relation to other requirements pertaining to the collection of information; and

30 (iii) with regard to information system development, security, and the use of information
31 technology resources;

32 (D) determine when and how to conduct public consultations;

33 (E) conduct a privacy impact assessment process for an agency activity affecting privacy that
34 involves more than one agency; and

35 (F) conduct any other aspect of the privacy impact assessment process.
36

37 (c) MANAGING THE PRIVACY IMPACT ASSESSMENT PROCESS.

38 (1) The Chief Privacy Officer shall determine the scope of each privacy impact assessment
39 process, including deciding whether a thorough or limited process is appropriate; which agency
40 activities affecting privacy should be included in which privacy impact assessment process; identify the
41 agency components that shall participate in the process; establish a timetable for the process; and
42 manage any public notice and public participation.

43 (2) Each privacy impact assessment process shall result in a final written report.

44 (3) If an agency activity affecting privacy involves classified information or other information
45 unsuitable for public disclosure under existing laws and Executive Orders, the agency shall disclose
46 publicly as much about the privacy impact assessment process as practicable.

47 (4) If in the judgment of the Chief Privacy Officer, it is not practical to complete a privacy
48 impact assessment process before an agency begins or significantly changes an activity that would
49 otherwise require a privacy impact assessment process, the Chief Privacy Officer may delay or

1 otherwise adjust the conduct of the process and the timing and form of public report in a suitable
2 manner. The Chief Privacy Officer shall provide public notice of any delay or adjustment on the
3 agency privacy website.

4 (5) The Chief Privacy Officer shall send to appropriate Committees of Congress a copy of each
5 interim and final written report on each major privacy impact assessment.

6
7 (d) ELEMENTS OF A PRIVACY IMPACT ASSESSMENT PROCESS.

8 (1) An agency conducting a thorough privacy impact assessment process shall, to the extent
9 practicable, include –

10 (A) an identification of risks to the agency from the processing of records, including a
11 description of ways to manage and to mitigate the risks and a justification for the final choices made
12 by the agency;

13 (B) an identification of information technology available to support the processing of records,
14 including a justification for the final choices made by the agency;

15 (C) an analysis of the risks and consequences of the activity for privacy of data subjects,
16 including expected uses and disclosures; a description of possible ways to mitigate the consequences
17 and risks; and a justification for the final choices made by the agency; and

18 (D) a description of efforts to seek public and stakeholder participation in the privacy impact
19 assessment process and a response by the agency to public and stakeholder comments.

20 (2) An agency conducting a limited privacy impact assessment process shall, to the extent practicable,
21 include –

22 (A) an explanation of the reasons that the agency decided to conduct a limited rather than a
23 thorough privacy impact assessment process;

24 (B) a description of the risks and consequences of processing of records for the agency and for
25 data subjects;

26 (C) a description of alternatives considered;

27 (D) a justification for the final choices made by the agency; and

28 (E) a summary of any public and stakeholder participation and comments.

29
30 (e) PUBLIC NOTICE AND PARTICIPATION. The Chief Privacy Officer of an agency shall,
31 to the extent practicable, provide for public notice of each privacy impact assessment process and for
32 public comment or other public participation in the process. The Chief Privacy Officer may provide
33 public notice through the privacy website of the agency or through the Federal Register.

34
35 (f) PUBLIC LAW 107-437. – An agency or component that completed the transition to this
36 Act shall not comply with section 208(b) of Public Law 107-437, 44 United States Code § 3501 note.

37
38 **Sec. 12. Exemptions**

39
40 (a) LIMITS ON ACCESS. – Nothing in this Act shall allow an individual a right of access
41 to a record or a disclosure history record, or a right of amendment of (1) any information compiled in
42 reasonable anticipation of a civil action or proceeding, (2) any classified information; (3) data or
43 information acquired by an agency under a pledge of confidentiality and used or disclosed for
44 exclusively statistical purposes pursuant to section 3572 of title 44, United States Code; (4) any
45 information created as testing or examination material used solely to determine individual
46 qualifications for appointment or promotion in the Federal service if disclosure would compromise
47 the objectivity or fairness of the testing or examination process; or (5) information that was exempt
48 from disclosure under section 552a of title 5, United States Code, as information collected prior to the

1 effective date of section 3 of the Privacy Act of 1974 (Public Law No. 93-579) under an implied
2 promise that the identity of the source would be held in confidence.

3
4 (b) PERSONNEL INVESTIGATIONS AND EVALUATIONS. – An agency is exempt from the
5 requirement in subsection (a) of section 4 to process only relevant and necessary information and
6 from the requirements in section 7 and section 8 to provide an individual a right of access, a right of
7 amendment, or a disclosure history record with respect to any information that would identify a
8 confidential source who furnished information to the Government under an express promise that the
9 identity of the source would be held in confidence if the information was created as –

10 (1) investigatory material solely for the purpose of determining suitability, eligibility, or
11 qualifications for Federal civilian employment, military service, Federal contracts, or access to
12 classified information.

13 (2) evaluation material to determine potential for promotion in the armed services.

14
15 (c) INVESTIGATORY MATERIAL FOR LAW ENFORCEMENT PURPOSES. –

16 (1) An agency is exempt from the requirement in subsection (a) of section 4 to process only
17 relevant and necessary information, and from the requirements in section 7 and section 8 to provide
18 an individual a right of access, a right of amendment, or a disclosure history record, for investigatory
19 information compiled for law enforcement purposes unless the individual is denied any rights,
20 benefits, privileges, or status that the individual would otherwise be entitled to by Federal law, or for
21 which the individual would otherwise be eligible, as a result of the maintenance of the information.

22 (2) Any right of access, right of amendment, or a disclosure history record in section 7 and
23 section 8 that an individual would have as a result of a denial of any rights, benefits, privileges, or
24 status as described in paragraph (1) of this subsection shall not apply to –

25 (A) the extent that the disclosure of the material would reveal the identity of a source who
26 furnished information to the Government under an express promise that the identity of the source
27 would be held in confidence;

28 (B) information exempt from disclosure pursuant to subsection (a)(5) of this section; or

29 (C) information that qualifies for exemption as criminal law enforcement information in
30 subsection (f).

31
32 (d) PROTECTIVE SERVICES. –An agency activity affecting privacy operated by an agency in
33 connection with providing protective services to the President of the United States or other
34 individuals pursuant to section 3056 of title 18, United States Code, is exempt from the requirement
35 in subsection (a) of section 4 to process only relevant and necessary information, and from the
36 requirements in section 7 and section 8 to provide an individual a right of access, a right of
37 amendment, or a disclosure history record to the extent that records in the agency activity affecting
38 privacy relate to those protective services.

39
40 (e) INTELLIGENCE AGENCIES. –

41 (1) An intelligence agency or component thereof defined as part of the Intelligence
42 Community pursuant to section 3003, title 50, United States Code is exempt from –

43 (A) the requirements to comply with subsections (a), (b), (c), and (d) of section 4; and

44 (B) the requirements in section 7 and section 8 to provide an individual a right of access, right
45 of amendment, or a disclosure history record.

46
47 (f) CRIMINAL LAW ENFORCEMENT AGENCIES. – A criminal law enforcement agency or
48 component thereof that performs as its principal function any activity pertaining to the enforcement
49 of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend

1 criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole
2 authorities, is exempt from the requirement to comply with subsections (a), (b), (c), and (d) of section
3 4, and from the requirements in section 7 and section 8 to provide an individual a right of access, a
4 right of amendment, or a disclosure history record with respect to any records that consist of –

5 (1) information compiled for the purpose of identifying individual criminal offenders and
6 alleged offenders and consisting only of identifying data and notations of arrests, the nature and
7 disposition of criminal charges, sentencing, confinement, release, and parole and probation status;

8 (2) information compiled for the purpose of a criminal investigation, including reports of
9 informants and investigators, and associated with an identifiable individual; or

10 (3) reports identifiable to an individual compiled at any stage of the process of enforcement of
11 the criminal laws from arrest or indictment through release from supervision.

12
13 (g) NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. – Any record subject to
14 this Act accepted by the National Archives of the United States as a record with sufficient historical or
15 other value to warrant its continued preservation by the United States Government pursuant to
16 section 2107 of title 44, United States Code, and that the Archivist of the United States processes
17 pursuant to section 2108 of title 44 United States Code, shall not be subject to any of the requirements
18 of this Act.

19
20 (h) GENERAL REQUIREMENTS. –

21 (1) When publishing a notice of an agency activity affecting privacy that includes a record
22 exempt or potentially exempt under provisions of this section, an agency shall, to the extent
23 practicable, describe the activities that qualify for the exemption and distinguish exempt and non-
24 exempt records and activities. The agency shall include in the notice the reasons the agency expects to
25 utilize the exemptions.

26 (2) In applying an exemption available under this section, an agency shall restrict application
27 of the exemption to those records and activities that include information that the exemption seeks to
28 protect.

29 (3) If an agency discloses a record exempt under this section from any provision to another
30 agency, the record shall continue to be exempt in the same manner and to the same extent as if the
31 disclosing agency continued to process the record. An agency transferring an exempt record shall
32 identify for the recipient agency the part of the record that qualifies for exemption and the nature and
33 scope of the exemption.

34
35 (i) WAIVERS. – An agency processing a record that qualifies for exemption in this section
36 may take one or more of the following actions –

37 (1) waive application of an exemption, in whole or in part, by including the waiver in the
38 description required in section 5(c) of an agency activity affecting privacy;

39 (2) issue a regulation defining when the agency may waive application of an exemption, in
40 whole or in part; and

41 (3) waive application of an exemption in whole or in part or on a case-by-case basis.

42 43 **Sec. 13. Criminal and Other Penalties**

44
45 (a) OFFENSES. –

46 (1) Any person who knowingly and willfully and in violation of this Act and under false
47 pretenses obtains a record that contains personally identifiable information shall be punished as
48 provided in subsection (b).

1 (2) Any officer, employee, contractor, grantee, or volunteer of an agency, or other person who
2 by virtue of employment, official position, or contract has possession of, or access to, a record that
3 contains personally identifiable information the disclosure of which is prohibited by this Act or by
4 rules or regulations established thereunder, and who knowing that disclosure of the record is so
5 prohibited, willfully discloses the material in any manner to any person or agency not entitled to
6 receive it, shall be punished as provided in subsection (b).

7
8 (b) PENALTIES. – A person described in subsection (a) shall –

9 (1) be fined not more than \$50,000, imprisoned not more than 1 year, or both;

10 (2) if the offense is committed with intent to sell, transfer, or use a record that contains
11 personally identifiable information for commercial advantage, personal gain, or malicious harm, be
12 fined not more than \$250,000, imprisoned not more than 10 years, or both.

13
14 (c) PUBLISHING. – Any officer or employee of any agency who willfully establishes or
15 maintains an agency activity affecting privacy without meeting the requirements in section 3 to
16 publish a description of the agency activity affecting privacy shall be guilty of a misdemeanor and
17 fined not more than \$5,000.

18
19 (d) ADVERSE PERSONNEL ACTIONS. – An officer or employee of an agency who processes
20 records in violation of this Act shall be subject to appropriate administrative discipline including,
21 when circumstances warrant, suspension from duty without pay or removal from office.

22 23 **Sec. 14. Government Contracts, Grants, and Cooperative Agreements.**

24
25 When an agency provides by a contract, grant, cooperative agreement, or otherwise for the conduct of
26 an agency activity affecting privacy to accomplish an agency function, whether in whole or in part, the
27 agency shall, consistent with its authority, cause the requirements of this Act to be applied to the
28 activity. The agency shall be responsible for any publication, notice, or rule required under this Act
29 with respect to that agency activity affecting privacy.

30 31 **Sec. 15. Matching.**

32
33 (a) MATCHING AGREEMENTS. –

34 (1) CONTENTS OF MATCHING AGREEMENTS. – A source agency shall not disclose a
35 record processed as part of an agency activity affecting privacy for use in a matching program except
36 pursuant to a written agreement between the source agency and the recipient agency or non-Federal
37 agency receiving the records, specifying –

38 (A) the purpose and legal authority for conducting the program;

39 (B) the justification for the program and the anticipated results, including a specific estimate
40 of any savings from the operation of the program;

41 (C) a description of the records that will be matched, including each data element that will be
42 used, the approximate number of records that will be matched, and the projected starting and
43 completion dates of the matching program;

44 (D) procedures for providing individualized notice at the time of application, and notice
45 periodically thereafter, to data subjects whose records are used in the activity that any information
46 provided by the data subjects may be subject to verification through matching programs;

47 (E) procedures for verifying information produced in the matching program as required by
48 this section;

1 (F) procedures for the retention and timely destruction of identifiable records created by a
2 recipient agency or non-Federal agency in the matching program;

3 (G) procedures for ensuring the administrative, technical, and physical security of the records
4 matched and the results of the programs;

5 (H) prohibitions on duplication and redisclosure of records imposed by the source agency on
6 the recipient agency or the non-Federal agency, except where duplication or redisclosure is required
7 by law or essential to the conduct of the matching program;

8 (I) procedures governing the use by the recipient agency or non-Federal agency of records
9 provided in a matching program by a source agency, including procedures governing return or
10 destruction of the records used in the program;

11 (J) information on assessments that have been made on the accuracy of the records that will be
12 used in the matching program;

13 (K) that the Comptroller General may have access to all records of a recipient agency or non-
14 Federal agency receiving the records as the Comptroller General deems necessary in order to monitor
15 or verify compliance with the agreement;

16 (L) a provision requiring revision or termination of the agreement if the need for,
17 circumstances relating to, or the law regarding any aspect of the matching agreement changes in a
18 material way during course of the agreement; and

19 (M) the expiration date for the agreement, which can be no later than five years after the
20 agreement took effect.

21 (2) CERTIFICATION OF MATCHING AGREEMENT. – No matching agreement shall take
22 effect unless the Chief Privacy Officer of the source agency certifies in writing that –

23 (A) the agreement complies with all requirements of this Act;

24 (B) the Chief Privacy Officer of the source agency consulted with the agency Inspector
25 General, Chief Information Officer, Chief Data Officer, and senior officials from the office providing
26 or using records for the matching program activity about the justification for the matching program;

27 (C) any findings of the agency Inspector General or the Government Accountability Office
28 relevant to the matching program were adequately taken into account in the agreement;

29 (D) any problems identified in previous matching programs between the same agencies were
30 adequately addressed;

31 (E) except for matching programs mandated by statute, in the judgment of the Chief Privacy
32 Officer of the source agency, the sharing of records pursuant to the matching agreement is financially
33 justified based on any relevant results of current or past matching programs; and

34 (F) except for matching programs mandated by statute, in the judgment of the Chief Privacy
35 Officer of the source agency, the matching program is in the public interest.

36 (3) PRIOR COMPLIANCE REQUIRED. – No source agency may enter into a second or
37 subsequent matching agreement unless –

38 (A) the recipient agency or non-Federal agency receiving the records certifies in writing that it
39 complied with the provisions of previous agreements; and

40 (B) the source agency has no reason to believe that the certification is inaccurate.

41 (4) POSTING. – A copy of each matching agreement and a copy of the certification of the
42 Chief Privacy Officer shall be posted on the website of the source agency and sent to the Director of
43 the Office of Management and Budget.

44 (5) EFFECTIVE DATE OF AGREEMENT. – No matching agreement shall be effective until
45 30 days after the date on which a copy is posted on the agency website.

46 (6) SECTION NOT AUTHORITY TO CONDUCT PROGRAMS. – Nothing in this section
47 may be construed to authorize –

48 (A) any matching programs not otherwise authorized by law; or

49 (B) disclosure of records for a matching program except to a Federal, State, or local agency.

1
2 (b) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS. –

3 (1) TIME FOR NOTICE AND RESPONSE. – In order to protect an individual whose record is
4 used in a matching program, no source agency or non-Federal agency using a record from a matching
5 program may suspend, terminate, reduce, or make a final denial of any financial assistance or payment
6 under a Federal benefit program to the individual, or take other adverse action against the individual,
7 as a result of information produced by the matching program, until –

8 (A)(i) the source agency has independently verified the information; or

9 (ii) the Chief Privacy Officer of the source agency determines in accordance with guidance
10 issued by the Director of the Office of Management and Budget that–

11 (I) the information is limited to identification and amount of benefits paid by the source
12 agency under a Federal benefit program; and

13 (II) the Chief Privacy Officer of the source agency has a high degree of confidence that the
14 information provided to the recipient agency is accurate;

15 (B) the individual receives a notice from the agency containing a statement of its findings and
16 informing the individual of the opportunity to contest the findings; and

17 (C) the expiration of –

18 (i) any time period established by statute or regulation for the individual to respond to that
19 notice; or

20 (ii) in the case of a program for which no the period is established, the end of the 30-day
21 period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided
22 to the individual.

23 (2) BASIS FOR ADVERSE ACTION. – The independent verification referred to in paragraph
24 (1)(A)(i) requires investigation and confirmation of specific information relating to an individual that
25 is used as a basis for an adverse action against the individual, including where applicable investigation
26 and confirmation of–

27 (A) the amount of any asset or income involved;

28 (B) whether the individual actually has or had access to the asset or income for the individual's
29 own use; and

30 (C) the period or periods when the individual actually had the asset or income.

31 (3) HEALTH AND SAFETY EXCEPTION. – Notwithstanding paragraph (1), an agency may
32 take any appropriate action otherwise prohibited by the paragraph if the agency determines that the
33 public health or public safety may be adversely affected or significantly threatened during any notice
34 period required by the paragraph.

35
36 **Sec. 16. Miscellaneous.**

37
38 (a) WAIVER. – A waiver of the rights provided under section 7 and section 8 of this Act is
39 against public policy and is void and unenforceable.

40
41 (b) SALE OF PERSONALLY IDENTIFIABLE INFORMATION. – An individual's name;
42 postal and electronic addresses; telephone numbers; and other personally identifiable information
43 may not be sold or rented by an agency unless specifically authorized by statute. This provision shall
44 not be construed to require the withholding of personally identifiable information otherwise
45 permitted to be made public.

46
47 (c) EFFECT OF OTHER LAWS. –

1 (1) FOIA EXEMPTIONS NOT APPLICABLE TO RIGHTS UNDER THIS ACT. – No agency
2 shall rely on any exemption contained in section 552 of title 5, United States Code, to withhold from
3 an individual any record that is otherwise accessible to the individual under the provisions of this Act.
4

5 (2) EXEMPTIONS UNDER THIS ACT NOT APPLICABLE TO FOIA. – No agency shall rely
6 on any exemption in this Act to withhold from an individual any record that is otherwise accessible to
7 the individual under the provisions of section 552 of title 5, United States Code.
8

9 (d) RIGHTS OF PARENTS AND GUARDIANS. – A parent, guardian, other person acting in
10 loco parentis, or person with a valid power of attorney who under applicable law has authority to act
11 on behalf of an individual may act on behalf of the individual under this Act.
12

13 (e) REPORT TO CONGRESS. – Each agency that proposes to establish or make a change in
14 an agency activity affecting privacy that significantly limits or otherwise alters the rights and
15 opportunities available to individuals under this Act, or that adds or significantly modifies an agency
16 designated disclosure shall provide adequate advance notice to appropriate Committees of Congress
17 and to the Office of Management and Budget.
18

19 (f) WEBSITE. – Each agency shall maintain a privacy website, with appropriate search,
20 indexing, and finding aids, that allows for the full search and downloading of text maintained on the
21 website. The website shall include –

22 (1) the notice for each current agency activity affecting privacy and any personally identifiable
23 information processing diagram prepared in accordance with section 9(d) of this Act.

24 (2) a complete history of all changes made in the past ten years to the notice of each agency
25 activity affecting privacy, including the full text of each prior published notice, an identification of all
26 changes, and date on which each change took effect;

27 (3) a complete list of all Federal Register notices, including all amendments, for each agency
28 activity affecting privacy, together with an electronic or digital link to each notice;

29 (4) the text of all system of records notices and amendments published under the Privacy Act
30 of 1974 for the ten-year period before completion of the agency transition to compliance with this
31 Act;

32 (5) information about, and to the extent practicable, a copy of each privacy impact assessment
33 report completed in the past twenty-years or currently being conducted;

34 (6) other information determined by the head of the agency or by the Chief Privacy Officer to
35 be helpful to the public in understanding agency privacy activities, the provisions of this Act, and the
36 exercise of privacy rights granted by this Act to individuals; and

37 (7) information about the agency's plans for transition from compliance with the Privacy Act
38 of 1974 to compliance with this Act.
39

40 (g) STATUTE OR TREATY. – The failure of an agency to identify a statute or treaty requiring
41 or specifically authorizing disclosure of a record in any notice or publication under this Act shall not
42 overcome any requirement or authorization to disclose the record as provided in the statute or treaty.
43

44 **Sec. 17. Agency Rules**

45 (a) AGENCY RULES. – In order to carry out the provisions of this Act, each agency that
46 maintains an agency activity affecting privacy shall promulgate rules, in accordance with the
47 requirements (including general notice) of section 553 of title 5, United States Code, that shall –
48

1 (1) establish procedures whereby an individual can be notified in response to the individual's
2 request if any agency activity affecting privacy identified by the individual contains a record pertaining
3 to him;

4 (2) define reasonable times, places, and requirements for authenticating the identity of a data
5 subject who requests a record or information pertaining to the data subject before the agency shall
6 make the record or information available to the data subject;

7 (3) establish procedures for the disclosure to a data subject upon request the data subject's
8 record;

9 (4) establish procedures for reviewing a request from a data subject for amendment of any
10 record or information, for making a determination on the request, for an appeal within the agency of
11 an initial adverse agency determination, and for whatever additional means may be necessary for a
12 data subject to be able to exercise fully the data subject's rights under this Act;

13 (5) describe any limits that apply to the exercise of rights under this Act as a result of
14 exemptions and including the name of any agency activity affecting privacy to which exemptions
15 apply;

16 (6) establish fees to be charged, if any, to a data subject for making a copy of records
17 requested under this Act, excluding the first 1000 pages of records provided on paper, any record
18 provided in electronic form or format, and the cost of search for and review of the records; and

19 (7) establish rules of conduct for persons involved in the design, development, conduct, or
20 maintenance of any agency activity affecting privacy, or in processing any personally identifiable
21 information, and instruct each person about the rules and the requirements of this Act and the
22 penalties for noncompliance.

23
24 (b) COMPILATION. – The Office of the Federal Register shall biennially compile and publish
25 on a public website available without charge the rules promulgated under this Act and agency
26 descriptions of agency activities affecting privacy published under section 4 of this Act, together with
27 appropriate search, indexing, and finding aids.

28 29 **Sec. 18. Civil Remedies.**

30
31 (a) REMEDY. – A data subject may bring a civil action against the agency, and the
32 district courts of the United States shall have jurisdiction in the matters under the provisions
33 of this section, whenever any agency –

34 (1) fails to comply with the data subject's request under section 7(a) or section 8(b)(2)
35 of this Act;

36 (2) decides after review not to amend the data subject's record in accordance with the
37 data subject's request under section 7(b) of this Act, or fails to make the review in conformity
38 with that section;

39 (3) fails to process any record concerning the data subject with sufficient accuracy,
40 relevance, timeliness, and completeness as is necessary to assure fairness in any
41 determination relating to the qualifications, character, rights, benefits, privileges, or status, of
42 the data subject that may be made on the basis of the record, and consequently a
43 determination is made which is adverse to the data subject; or

44 (4) fails to comply with any other provision of this Act, or any rule promulgated
45 thereunder, in a way that has an adverse effect, including mental or emotional distress, on the
46 data subject.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45

(b) APPEAL.

(1) INJUNCTION TO PROVIDE RECORDS. – In any suit brought with respect to a failure described in subsection (a)(1), the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld. The court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in section 12 of this Act. The burden is on the agency to sustain its action.

(2) INJUNCTION TO AMEND RECORDS. – In any suit brought with respect to a decision or failure described in subsection (a)(2), the court may order the agency to amend the data subject’s record in accordance with the data subject’s request or in any other way as the court may direct. The court shall determine the matter de novo.

(3) DAMAGES AND COSTS. – In any suit brought with respect to a decision or failure described in subsection (a)(3) or (a)(4) in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the data subject for –

(A) provable damages, including mental or emotional distress, sustained by the data subject as a result of the refusal or failure or \$1000, whichever is greater, but in any class action, the court may reduce the damage award if the total damages are excessive or otherwise unwarranted; and

(B) the costs of the action together with reasonable attorney fees and other litigation costs as determined by the court;

(4) VENUE AND STATUTE OF LIMITATIONS. – An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or in which the complainant has a principal place of business, or in which the agency headquarters are located, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that if an agency materially and willfully misrepresented any information required under this Act to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this Act, the action may be brought at any time within two years after discovery by the individual of the misrepresentation.

Sec. 19. Administrative Remedy.

(a) COMPLAINT. –

(1) Any person may file with the Chief Privacy Officer of the agency a complaint setting forth specific facts alleging that an agency failed to comply in a material way with this Act, including any provision regulating –

(A) publication of a timely and accurate description of an agency activity affecting privacy;

(B) a properly defined and adopted agency defined disclosure;

(C) a meaningful and timely privacy impact assessment process;

(D) matching programs; or

1 (E) any other action specified in this Act.

2 (3) The Chief Privacy Officer of the agency shall –

3 (A) acknowledge receipt of a complaint under this subsection in writing within ten
4 days;

5 (B) within 90 days, either (i) reject a complaint that lacks sufficient specificity to
6 adequately identify or support the allegations in the complaint or that lacks merit, and
7 promptly notify the complainant of the right to appeal under this section, or (ii) if any
8 allegations in the complaint are found to be meritorious, promptly inform the complainant of
9 that decision and undertake reasonable steps to correct any identified deficiencies.

10
11 (b) JUDICIAL REVIEW. –

12 (1) ACTIONS AUTHORIZED. – A complainant whose complaint under this section –

13 (A) was denied in whole or in part by the agency;

14 (B) was determined to be meritorious, but on which the agency unreasonably delayed
15 corrective actions; or

16 (C) did not receive a substantive response from the agency within three months after filing the
17 complaint –

18 may bring a civil action against the agency to obtain judicial review pursuant to sections 701 through
19 705 of title 5, United States Code, and the district courts of the United States shall have jurisdiction in
20 the matter.

21 (2) VENUE. – An action under this section may be brought in the district court of the United
22 States in the district in which the complainant resides, or has a principal place of business, or in which
23 the agency headquarters are located, or in the District of Columbia, without regard to the amount in
24 controversy.

25 (3) ORDERS. – The court may order the agency to correct any material failure to comply with
26 this Act.

27 (4) COSTS. – The court may assess against the United States the costs of the action
28 together with reasonable attorney fees and other litigation costs as determined by the court
29 in any case under this section in which the complainant has substantially prevailed.

30
31 **Sec. 20. Effective Date and Transition.**

32
33 (a) EFFECTIVE DATE. – This Act shall take effect ten days after the date of enactment.
34 Agencies shall comply with this Act as provided in this section.

35
36 (b) TRANSITION. – Within one year after the effective date of this Act, each agency subject
37 to the Privacy Act of 1974 shall prepare a transition plan for changing its privacy compliance activities
38 from section 552a of title 5, United States Code, to this Act. Each agency shall send a copy of its plan
39 to the Director of the Office of Management and Budget and shall post a copy of its plan on the
40 agency's privacy website.

41
42 (c) TRANSITION PLAN. – The transition plan –

43 (1) shall establish a date when all components of the agency will comply with this Act, not to
44 exceed five years from the date of enactment;

45 (2) shall provide for the promulgation of agency rules required by this Act before any part of
46 the agency completes the transition;

1 (3) shall provide for publication of a notice disclosing the date of transition in the Federal
2 Register at least 30 days before the date when all or part of the agency completes the transition to this
3 Act;

4 (4) shall, not less frequently than every six months until the transition for the entire agency is
5 complete, provide for public notice of the progress of the agency's transition on the agency's privacy
6 website;

7 (5) may provide different transition dates for different agency components.
8

9 (d) PRIVACY IMPACT ASSESSMENT DURING TRANSITION. – (1) An agency may choose
10 not conduct a privacy impact assessment process as provided in section 11 before it first establishes an
11 agency activity affecting privacy during the transition to compliance with this Act if the agency
12 determines that –

13 (A) a recent privacy impact assessment substantially accomplished the purposes set out in
14 section (11)(a) for the agency activity affecting privacy; or

15 (B) the agency activity affecting privacy only requires a limited privacy impact assessment and
16 the activity is comparable to an activity covered by a privacy impact assessment conducted during the
17 five years before the initial establishment of the activity.

18 (2) In determining priorities and allocating resources for privacy impact assessment processes
19 during the transition, the agency shall give priority to new agency activities affecting privacy, to
20 activities that are likely involve greater risk to the agency or to data subjects, and to any novel or
21 innovative applications of technology.
22

23 (e) TERMINATION. – An agency or agency component that completes the transition from
24 the section 552a of title 5, United States Code, to this Act shall terminate compliance with section
25 552a of title 5, United States Code, on the transition date for the agency or agency component.
26

27 (f) OFFICE OF MANAGEMENT AND BUDGET. –

28 (1) The Director of the Office of Management and Budget shall issue guidance to agencies
29 regarding the transition from section 552a of title 5, United States Code, to this Act.

30 (2) Upon the request of an agency, the Director of the Office of Management and Budget may
31 allow the agency to amend its transition plan and to take additional time to complete the transition.
32 No extension may be granted beyond seven years from the date of enactment of this Act.

33 (3) Until the transition is complete for all agencies, the Director of the Office of Management
34 and Budget shall report annually to the Congress and to the public on the government's progress in
35 transitioning to compliance with this Act.
36

37 (g) LITIGATION. – Any litigation initiated under the section 552a of title 5, United States
38 Code, shall be unaffected by this Act and shall continue under the provisions of the section 552a of
39 title 5, United States Code, notwithstanding whether the agency completed its transition to this Act.