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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 3. Definitions.

In this Act:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 4. General Processing Requirements.

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

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

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

(1) the authority for the collection;

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

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

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

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

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

(f) FIRST AMENDMENT. – No agency shall process a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute, or by the individual, or unless pertinent to and within the scope of an authorized law enforcement activity.
(g) LEGAL PROCESS. – Each agency shall make reasonable efforts to serve notice on a data subject when any personally identifiable information about the data subject is made available to any person under compulsory legal process when the process becomes a matter of public record.

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

Sec. 5. Agency Activity Affecting Privacy.

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

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

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

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

1. the name of the activity, the scope of the activity, each principal substantive purpose that the activity supports, and the authority for the activity, including any related information collection requests approved under the Paperwork Reduction Act;
2. the name of the agency component primarily responsible for the activity, the principal postal, electronic mail, and website addresses of that component, and the name of other agency components that significantly participate in the activity;
3. the categories of data subjects about whom records are processed as part of the activity;
4. the categories of records processed in the activity;
5. the principal information technologies employed, including any novel or innovative applications of technology; any automated decision making; any processing of records using artificial intelligence; any algorithmic development, analysis, or application; or any similar activities with the potential to affect the rights or interests of data subjects;
6. each agency designated disclosure applicable to records processed as part of the activity, including a good faith effort to list agency designated disclosures in the approximate order in which they are likely to be used, with the most used disclosure listed first;
7. the categories of sources of records in the activity, including any commercial, governmental, or other sources that the agency routinely reviews, consults, or otherwise uses to carry out the activity;
(8) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of records in the activity, including the name and location of records disposal schedules covering any of the records;

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 6. Allowable Uses and Disclosures.

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

(1) use or withhold from use a record as otherwise provided by statute; or
(2) withhold a record used for one agency function from another agency function.

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

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

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

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

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

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

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

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

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

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

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

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

(A) the agency believes in good faith that –

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

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

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

(7) CONGRESS. – The disclosure is to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, or any joint committee of Congress or subcommittee of any the joint committee.
(8) WRITTEN INQUIRY TO MEMBER OF CONGRESS. – The disclosure is to a Member of Congress in response to a written inquiry by the Member of Congress after the Member of Congress receives a written request from the data subject pertaining to or concerning a matter contained in the record.

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

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

(11) COURTS AND LITIGATION. – The disclosure –
(A) is pursuant to the order of a court of competent jurisdiction;
(B) occurs in a filing made in a court of competent jurisdiction pursuant to the rules of that court;
(C) is to a party in litigation with the agency, is authorized by the rules or order of the court or adjudicative body conducting the proceeding before which the litigation is pending, and a rule, order, or a signed written agreement, limits use of the disclosed record to the purpose of conducting the litigation; or
(D)(i) is to a party, or potential party, to litigation with the agency, or to the party’s authorized representative, or to an independent mediator, in connection with settlement discussions; and
(ii) the disclosure of the record is limited to the purposes of the settlement negotiations by (I) a rule or order of the court or adjudicative body conducting the proceeding, or (II) a written agreement signed by the parties.

(12) DATA BREACH RESPONSE. – The disclosure is –
(A) for the purpose of responding to a suspected or confirmed data breach that involves a risk of harm to an individual or a data system;
(B) approved by –
(i) the head of the agency;
(ii) the Chief Privacy Officer of the agency;
(iii) a senior agency official designated under a written agency data breach response plan; or
(iv) the Federal Chief Privacy Officer;
(C) of records from an agency activity affecting privacy that an agency official supervising the data breach response determines are (i) likely to be relevant to the purpose of this paragraph; and (ii) made to an agency, entity, or other person for which the official approving the disclosure has reason to believe may be able to assist in identifying the existence or scope of a data breach or in responding to the data breach either by providing a remedy for an individual who may have been affected by the data breach or by assisting with protection of a data system; and
(D) pursuant to a contract or agreement limiting the use of all data disclosed to the purpose of the disclosure and requiring either the prompt return or destruction of all data disclosed when the agency determines that the purposes of the disclosure are fulfilled.

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

Appendix 1 - 9
(e) MINIMIZE ALLOWABLE DISCLOSURES. – When disclosing a record pursuant to an allowable disclosure in subsection (d), an agency shall make a good faith effort to disclose the minimum amount of personally identifiable information that will accomplish the purpose of the disclosure.

(f) PROCEDURAL REQUIREMENTS FOR AGENCY DESIGNATED DISCLOSURES.

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

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

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

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

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

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

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

(3) MINIMIZING DISCLOSURE. –

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

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

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

(g) OMB GUIDANCE. –

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

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

(h) LIMITS. – Except as otherwise provided by law, nothing in this Act requires an agency to disclose a record to anyone other than the data subject or to a parent, guardian, or other person identified in section 16(d).
Sec. 7. Access to and Amendment of Records.

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

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

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

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

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

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

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

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

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

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

(B) inform the data subject of –

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

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

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

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

Appendix 1 - 11
Sec. 8. Disclosure History

(a) ACCURATE DISCLOSURE HISTORY REQUIRED. – Each agency, with respect to each
agency activity affecting privacy, shall except for uses made under section 6(a) and disclosures made
under section 6(d)(1), keep or maintain the ability to create upon request an accurate history of –
(1) the date, nature, and purpose of each disclosure of a record to any person or to another
agency made pursuant to an agency designated disclosure; and
(2) the name and address of the person or agency to whom the disclosure is made;
(b) RETENTION, AVAILABILITY, AND NOTICE OF DISCLOSURE HISTORY. – Each
agency shall –
(1) keep or maintain the ability to create upon request a disclosure history for at least five
years after the disclosure or for the life of the record, whichever is longer;
(2) except for disclosures made under section 6(d)(2), (3), (4) and (5), make the disclosure
history available to the data subject upon a request made pursuant to the access procedure described
in section 7(a); and
(3) inform any person or other agency about any amendment or statement of disagreement
made in accordance with section 7 of any record previously disclosed to the person or agency if a
disclosure history is available, if the data subject who requested the amendment or submitted a
statement of disagreement asks that the amendment or statement be disclosed.

Sec. 9. Chief Privacy Officer.

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

(b) DUTIES. – The Chief Privacy Officer for an agency shall –
(1) have agency-wide responsibility for privacy and for compliance with fair information
practices;
(2) have agency-wide responsibility for overseeing agency compliance with Federal laws,
regulations, and policies relating to privacy, including primary responsibility for implementation of
this Act;
(3) participate in identifying and addressing privacy risks throughout the agency;
(4) have responsibility for agency privacy impact assessments as provided in section 11;
(5) have a central role in the agency’s development and evaluation of legislative, regulatory,
and other policy proposals relating to or affecting the privacy of personally identifiable information;
and
(6) approve the publication of the description of each agency activity affecting privacy,
including each agency designated disclosure, prior to publication for comment and before the
description and the agency designated disclosure becomes final.

(c) NOTICES. – The Chief Privacy Officer shall, to the extent practicable, standardize
elements and terminology of notices of agency activities affecting privacy, including agency designated
disclosures.
(d) Personally Identifiable Information Processing Diagram. – The Chief Privacy Officer shall, to the extent practicable, maintain on the agency privacy website for each major agency activity affecting privacy a current personally identifiable information processing diagram or equivalent document that visually depicts the collection, use, and disclosure of personal information and that shows the principal sources of information, the principal internal users of the personal information, the principal purposes for which the agency collects and discloses personal information, and the recipients of the disclosures.

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

(1) consult with the Chief Information Officer of the agency; and

(2) report from time to time directly to the head of the agency.

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

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

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

(b) DUTIES. – The Office of the Federal Chief Privacy Officer shall –

(1) have responsibility for preparing Office of Management Budget guidance under this Act;

(2) provide notice and opportunity for public comment for the guidance;

(3) assist and direct agencies with the transition from compliance with the Privacy Act of 1974 to compliance with this Act;

(4) oversee agency compliance with this Act and provide continuing assistance to agencies with the implementation of this Act; and

(5) have responsibility for advising the Director on all privacy matters.

Sec. 11. Privacy Impact Assessment Process.

(a) PURPOSE. – The purposes of the privacy impact assessment process are –

(1) to inform agency decisions for the life cycle of agency activities affecting privacy, including planning, design, implementation, and conduct, in a manner consistent with other Federal information resources management policies, principles, standards, and guidelines;

(2) to identify significant risks to the agency and significant consequences for the privacy of data subjects from the conduct of agency activities affecting privacy;

(3) to seek and implement ways to minimize significant risks and consequences prior to establishing or modifying an agency activity affecting privacy while providing for the efficient and effective conduct of agency responsibilities;

(4) to provide that agency processing of personal information minimizes the processing of personally identifiable information, maximizes fairness, includes appropriate due process protections, and generally complies with fair information practices;
(5) to provide to the extent practicable an opportunity for public comment in the planning
and design of an agency activity affecting privacy;
(6) to complete the process, to the extent practicable, before the agency makes final decisions
about the design of an agency activity affecting privacy; and
(7) to document the conduct of the process with a written report.

(b) PROCESS. –
(1) Each agency shall conduct either a thorough or a limited privacy impact assessment
process for new or significantly modified agency activities affecting privacy and for new or
significantly revised matching programs.
(2) In determining whether to conduct a thorough or a limited privacy impact assessment
process, an agency shall consider using a thorough assessment when agency activities affecting privacy
are reasonably likely to have one or more of these characteristics:
   (A) affect a large number of data subjects;
   (B) involve determinations of eligibility for rights, benefits, privileges, or status;
   (C) employ or propose to employ any novel or innovative applications of technology;
   (D) present significant risks to the agency or significant consequences for the privacy
   of data subjects;
   (E) involve the routine collection of records from sources outside the Federal
government or the routine disclosure of records outside the Federal government; or
   (F) result in significant new mergers of previously separate government databases.
(3) The Director of the Office of Management and Budget shall issue guidance to help
agencies –
   (A) decide whether to conduct either a thorough or a limited privacy impact assessment
   process;
   (B) establish priorities for conducting privacy impact assessment processes;
   (C) address privacy –
   (i) as part of the information and information system life cycles;
   (ii) in relation to other requirements pertaining to the collection of information; and
   (iii) with regard to information system development, security, and the use of information
   technology resources;
   (D) determine when and how to conduct public consultations;
   (E) conduct a privacy impact assessment process for an agency activity affecting privacy that
   involves more than one agency; and
   (F) conduct any other aspect of the privacy impact assessment process.

(c) MANAGING THE PRIVACY IMPACT ASSESSMENT PROCESS.
(1) The Chief Privacy Officer shall determine the scope of each privacy impact assessment
process, including deciding whether a thorough or limited process is appropriate; which agency
activities affecting privacy should be included in which privacy impact assessment process; identify the
agency components that shall participate in the process; establish a timetable for the process; and
manage any public notice and public participation.
(2) Each privacy impact assessment process shall result in a final written report.
(3) If an agency activity affecting privacy involves classified information or other information
unsuitable for public disclosure under existing laws and Executive Orders, the agency shall disclose
publicly as much about the privacy impact assessment process as practicable.
(4) If in the judgment of the Chief Privacy Officer, it is not practical to complete a privacy
impact assessment process before an agency begins or significantly changes an activity that would
otherwise require a privacy impact assessment process, the Chief Privacy Officer may delay or
otherwise adjust the conduct of the process and the timing and form of public report in a suitable manner. The Chief Privacy Officer shall provide public notice of any delay or adjustment on the agency privacy website.

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

(d) ELEMENTS OF A PRIVACY IMPACT ASSESSMENT PROCESS.

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

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

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

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

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

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

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

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

(C) a description of alternatives considered;

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

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

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

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

Sec. 12. Exemptions

(a) LIMITS ON ACCESS. – Nothing in this Act shall allow an individual a right of access to a record or a disclosure history record, or a right of amendment of (1) any information compiled in reasonable anticipation of a civil action or proceeding, (2) any classified information; (3) data or information acquired by an agency under a pledge of confidentiality and used or disclosed for exclusively statistical purposes pursuant to section 3572 of title 44, United States Code; (4) any information created as testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service if disclosure would compromise the objectivity or fairness of the testing or examination process; or (5) information that was exempt from disclosure under section 552a of title 5, United States Code, as information collected prior to the
effective date of section 3 of the Privacy Act of 1974 (Public Law No. 93-579) under an implied
promise that the identity of the source would be held in confidence.

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

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

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

(c) INVESTIGATORY MATERIAL FOR LAW ENFORCEMENT PURPOSES. –

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

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

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

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

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

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

(e) INTELLIGENCE AGENCIES. –

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

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

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

(f) CRIMINAL LAW ENFORCEMENT AGENCIES. – A criminal law enforcement agency or
component thereof that performs as its principal function any activity pertaining to the enforcement
of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend
criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole
authorities, is exempt from the requirement to comply with subsections (a), (b), (c), and (d) of section
4, and from the requirements in section 7 and section 8 to provide an individual a right of access, a
right of amendment, or a disclosure history record with respect to any records that consist of –
(1) information compiled for the purpose of identifying individual criminal offenders and
alleged offenders and consisting only of identifying data and notations of arrests, the nature and
disposition of criminal charges, sentencing, confinement, release, and parole and probation status;
(2) information compiled for the purpose of a criminal investigation, including reports of
informants and investigators, and associated with an identifiable individual; or
(3) reports identifiable to an individual compiled at any stage of the process of enforcement of
the criminal laws from arrest or indictment through release from supervision.

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

(h) GENERAL REQUIREMENTS. –
(1) When publishing a notice of an agency activity affecting privacy that includes a record
exempt or potentially exempt under provisions of this section, an agency shall, to the extent
practicable, describe the activities that qualify for the exemption and distinguish exempt and non-
exempt records and activities. The agency shall include in the notice the reasons the agency expects to
utilize the exemptions.
(2) In applying an exemption available under this section, an agency shall restrict application
of the exemption to those records and activities that include information that the exemption seeks to
protect.
(3) If an agency discloses a record exempt under this section from any provision to another
agency, the record shall continue to be exempt in the same manner and to the same extent as if the
disclosing agency continued to process the record. An agency transferring an exempt record shall
identify for the recipient agency the part of the record that qualifies for exemption and the nature and
scope of the exemption.

(i) WAIVERS. – An agency processing a record that qualifies for exemption in this section
may take one or more of the following actions –
(1) waive application of an exemption, in whole or in part, by including the waiver in the
description required in section 5(c) of an agency activity affecting privacy;
(2) issue a regulation defining when the agency may waive application of an exemption, in
whole or in part; and
(3) waive application of an exemption in whole or in part or on a case-by-case basis.

Sec. 13. Criminal and Other Penalties

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

(b) PENALITIES. – A person described in subsection (a) shall –
(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
(2) if the offense is committed with intent to sell, transfer, or use a record that contains
personally identifiable information for commercial advantage, personal gain, or malicious harm, be
fined not more than $250,000, imprisoned not more than 10 years, or both.

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

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


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

Sec. 15. Matching.

(a) MATCHING AGREEMENTS. –
(1) CONTENTS OF MATCHING AGREEMENTS. – A source agency shall not disclose a
record processed as part of an agency activity affecting privacy for use in a matching program except
pursuant to a written agreement between the source agency and the recipient agency or non-Federal
agency receiving the records, specifying –
(A) the purpose and legal authority for conducting the program;
(B) the justification for the program and the anticipated results, including a specific estimate
of any savings from the operation of the program;
(C) a description of the records that will be matched, including each data element that will be
used, the approximate number of records that will be matched, and the projected starting and
completion dates of the matching program;
(D) procedures for providing individualized notice at the time of application, and notice
periodically thereafter, to data subjects whose records are used in the activity that any information
provided by the data subjects may be subject to verification through matching programs;
(E) procedures for verifying information produced in the matching program as required by
this section;
(F) procedures for the retention and timely destruction of identifiable records created by a
recipient agency or non-Federal agency in the matching program;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) disclosure of records for a matching program except to a Federal, State, or local agency.
(b) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS. –
(1) TIME FOR NOTICE AND RESPONSE. – In order to protect an individual whose record is used in a matching program, no source agency or non-Federal agency using a record from a matching program may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to the individual, or take other adverse action against the individual, as a result of information produced by the matching program, until –
(A)(i) the source agency has independently verified the information; or
(ii) the Chief Privacy Officer of the source agency determines in accordance with guidance issued by the Director of the Office of Management and Budget that –
(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and
(II) the Chief Privacy Officer of the source agency has a high degree of confidence that the information provided to the recipient agency is accurate;
(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest the findings; and
(C) the expiration of –
(i) any time period established by statute or regulation for the individual to respond to that notice; or
(ii) in the case of a program for which no the period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.
(2) BASIS FOR ADVERSE ACTION. – The independent verification referred to in paragraph (1)(A)(i) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of –
(A) the amount of any asset or income involved;
(B) whether the individual actually has or had access to the asset or income for the individual’s own use; and
(C) the period or periods when the individual actually had the asset or income.
(3) HEALTH AND SAFETY EXCEPTION. – Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by the paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by the paragraph.

**Sec. 16. Miscellaneous.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 17. Agency Rules

(a) AGENCY RULES. – In order to carry out the provisions of this Act, each agency that maintains an agency activity affecting privacy shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of title 5, United States Code, that shall –
(1) establish procedures whereby an individual can be notified in response to the individual’s request if any agency activity affecting privacy identified by the individual contains a record pertaining to him;
(2) define reasonable times, places, and requirements for authenticating the identity of a data subject who requests a record or information pertaining to the data subject before the agency shall make the record or information available to the data subject;
(3) establish procedures for the disclosure to a data subject upon request the data subject’s records;
(4) establish procedures for reviewing a request from a data subject for amendment of any record or information, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for a data subject to be able to exercise fully the data subject’s rights under this Act;
(5) describe any limits that apply to the exercise of rights under this Act as a result of exemptions and including the name of any agency activity affecting privacy to which exemptions apply;
(6) establish fees to be charged, if any, to a data subject for making a copy of records requested under this Act, excluding the first 1000 pages of records provided on paper, any record provided in electronic form or format, and the cost of search for and review of the records; and
(7) establish rules of conduct for persons involved in the design, development, conduct, or maintenance of any agency activity affecting privacy, or in processing any personally identifiable information, and instruct each person about the rules and the requirements of this Act and the penalties for noncompliance.

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

Sec. 18. Civil Remedies.

(a) REMEDY. – A data subject may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this section, whenever any agency –
(1) fails to comply with the data subject’s request under section 7(a) or section 8(b)(2) of this Act;
(2) decides after review not to amend the data subject’s record in accordance with the data subject’s request under section 7(b) of this Act, or fails to make the review in conformity with that section;
(3) fails to process any record concerning the data subject with sufficient accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, benefits, privileges, or status, of the data subject that may be made on the basis of the record, and consequently a determination is made which is adverse to the data subject; or
(4) fails to comply with any other provision of this Act, or any rule promulgated thereunder, in a way that has an adverse effect, including mental or emotional distress, on the data subject.
(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
(E) any other action specified in this Act.

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

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

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

(b) JUDICIAL REVIEW. –

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

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

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

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

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

(2) VENUE. – An action under this section may be brought in the district court of the United States in the district in which the complainant resides, or 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.

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

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

Sec. 20. Effective Date and Transition.

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

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

(c) TRANSITION PLAN. – The transition plan –

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

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

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

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

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

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

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

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

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

(f) OFFICE OF MANAGEMENT AND BUDGET. –

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

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

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

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