U.S. GOVERNMENT PRIVACY
Essential Policies and Practices for Privacy Professionals
Second Edition

Deborah Kendall, CIPP/US, CIPP/G, Executive Editor

An IAPP Publication
Contents

Acknowledgments ................................................................. ix
Richard Soule, CIPP/US, CIPP/E

Introduction ........................................................................ xi
J. Trevor Hughes, CIPP

CHAPTER ONE
隐私原则和定义

隐私基本原则 ................................................................. 1
解析政府隐私在美国 ......................................................... 2
隐私定义 .......................................................................... 4
隐私和信任 ...................................................................... 5
美国联邦和州的隐私权利 .................................................. 7
联邦隐私计划 .................................................................... 7
引导原则的隐私信息 ......................................................... 8
影响技术的隐私 .............................................................. 14
结论 ................................................................................. 14

CHAPTER TWO
隐私法案和电子政府法案

隐私法案 .......................................................................... 17
电子政府法案 .................................................................... 29
结论 ................................................................................. 40
CHAPTER THREE
Other Laws and Regulations Focused on Government Agencies that Affect Their Privacy Practices

The Consolidated Appropriations Act of 2005 .......................................................... 43
The Federal Information Security Management Act .................................................. 45
The Freedom of Information Act (FOIA) ................................................................. 54
Paperwork Reduction Act (PRA) of 1995................................................................. 63
The Data Quality Act ............................................................................................... 65
Federal Open Meetings Laws .................................................................................. 67
Open Government Directive ...................................................................................... 70
Confidential Information Protection and Statistical Efficiency Act .......................... 72
Controlled Unclassified Information (CUI) Office Notice 2011-01:
Initial Implementation Guidance for Executive Order 13556 ................................. 73
Federal Agency Data Mining Reporting Act of 2007 .................................................. 74
Conclusion ................................................................................................................ 76

CHAPTER FOUR
Privacy and the Federal Government Intelligence Community

The Federal Intelligence Community and the Information Sharing Environment (ISE) ........... 81
Office of the Director of National Intelligence (ODNI) ............................................. 84
Implementing Recommendations of the 9/11 Commission Act of 2007 ......................... 85
Conclusion ................................................................................................................ 87

CHAPTER FIVE
Laws Affecting Both the Public and Private Sectors and Laws that Compel Disclosure of
Information to the Government

Laws with Privacy Implications for Private Industry and Government Agencies .................. 89
Laws that Compel Disclosure of Information to the Government .................................. 103
Conclusion ................................................................................................................ 112

CHAPTER SIX
Privacy Program Development and Organization

Program Development ............................................................................................... 115
NIST Risk Management Framework .......................................................................... 118
Program Management ............................................................................................... 123
Federal Agency Privacy Policies and Procedures ....................................................... 127
Protecting PII .............................................................................................................. 142
U.S. Government Workforce Management ............................................................... 145
Conclusion ................................................................................................................ 149
As the federal government collects increasing amounts of data in the Information Age, federal privacy professionals must learn and know the requirements of the Privacy Act of 1974 and the E-Government Act of 2002. These two statutes are the cornerstones for privacy protection within the nation when the U.S. government collects personally identifiable information (PII). Along with a good records management program, these laws and policies govern the collection and use of personal data from initial induction to final destruction.

1. The Privacy Act

Revised by Alexander C. Tang, CIPP/US, CIPP/G

The Privacy Act (P.L. 93-579, 5 U.S.C. § 552a) has guided the privacy practices of U.S. federal agencies since its passage. This landmark legislation can be seen as an access statute, which calls for certain Fair Information Practices (FIPs) and requires, in most instances, public notice of the types of personal data (i.e., PII) to be collected, processed, stored and used by a federal agency “system of records.” Through later amendment, the statute also requires disclosure of matching programs among agencies when the results of the match might affect the receipt of a government benefit. It ruled the policy landscape of federal privacy for nearly 30 years until the passage of the E-Government Act of 2002 and its requirements for privacy impact assessments (PIAs) for electronic information collection activities and website privacy policies.

While scholars continue to debate whether U.S. privacy law has a foundation in the U.S. Constitution, the preamble of the Privacy Act asserts that “the right to privacy is a personal and fundamental right protected by the Constitution of the United States,” and establishes clear responsibilities for federal systems with respect to privacy.

The original text for this chapter was developed by Erika L. McCallister, CIPP/US, CIPP/G, Stuart S. Shapiro, CIPP/US, CIPP/G and David Weitzel, CIPP/US, CIPP/G. New content for this revised edition was contributed by Alexander C. Tang, CIPP/US, CIPP/G and Rebecca J. Richards, CIPP/US, CIPP/G, whose contributions are noted throughout the sections of the chapter.
The Privacy Act also establishes the statutory foundation for the application of modern FIPs to federal government operations by implementing the 1973 code discussed in Chapter 1. Among other things, the Privacy Act requires agencies to:

- Limit PII collection to that which is “relevant and necessary”
- Collect PII directly from the individual whenever possible
- Maintain the accuracy, currency and completeness of PII
- Limit disclosure of PII to those who need access for proper purposes
- Allow access to and correction of PII
- Secure systems containing PII

1.1 Definitions under the Privacy Act

The Privacy Act provides the following key definitions:

- **Agency**: “[l]cludes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.”
- **Individual**: A “citizen of the United States or an alien lawfully admitted for permanent residence.”
- **Record**: “Any item, collection, or grouping of information about an individual that is maintained by an agency. . . and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”
The Privacy Act and the E-Government Act

- **System of Records:** “A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”
- **Routine Use:** “[T]he use of [a] record for a purpose which is compatible with the purpose for which it was collected.”
- **Matching Program:** “[A]ny computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of . . . establishing or verifying the eligibility of, or continuing compliance . . . 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 recouping payments or delinquent debts under such . . . programs, or [any computerized comparison of] two or more automated Federal personnel or payroll systems of records or [any such system] with non-Federal records.”

Several key aspects of the Privacy Act are:

- The law applies to U.S. citizens and legal permanent resident aliens only. However, some agencies have implemented policies that require them to protect the privacy of non-citizens in the same way that they protect the privacy of U.S. citizens or legal permanent resident aliens under the Privacy Act. For example, at the Department of Homeland Security (DHS), any PII that is collected, used, maintained, and/or disseminated in connection with a mixed system is treated as a system of records subject to the Privacy Act. A mixed system is a system that contains records both on U.S. citizens and legal permanent residents as well as non-citizens.2
- The law applies only to records in a system of records that are retrieved by a name or some other identifying number or symbol, such as a Social Security number. Some systems in the federal government collect information on individuals, but retrieve the information in other ways, such as a case number that cannot be linked directly to an individual. In such instances, the records are not a system of records under the definition provided by the Privacy Act. Federal government privacy professionals should work with their legal counsel to confirm which records are systems of records within their agency’s systems.
- There have been calls for updating the Privacy Act. The Privacy Act was enacted many years ago, and, since the law was passed, information technology has changed significantly. It can be very challenging to apply the Privacy Act to the kinds of technology and systems environments that exist today. Federal government privacy professionals should take care to consider the original intent of the Privacy Act when working to uphold the law’s provisions in their work.
1.2 Data Quality and Security

The Privacy Act requires agencies to ensure the quality of PII to provide fairness to the individual. It is expected that the degree of data quality required will vary with the intended use of the PII. The relevant factors for PII quality are accuracy (sufficiently correct), timeliness (sufficiently up-to-date) and completeness (sufficient information).

The agency must make reasonable efforts to ensure that Privacy Act records meet these requirements (and that such records are relevant for agency purposes) before disseminating them to anyone other than another agency or under the Freedom of Information Act (FOIA).

The act also mandates that agencies establish appropriate administrative, technical and physical safeguards to ensure security and confidentiality of the PII and to protect against anticipated threats or hazards to the security or integrity of such PII. The act does not specify the safeguards to be adopted, which are prescribed by other laws, regulations and policies governing information security and records management within the federal government (e.g., Federal Information Security Management Act [FISMA] guidance issued by the Office of Management and Budget [OMB], National Institute of Standards and Technology [NIST], DHS and National Archives and Records Administration [NARA]).

1.3 SORN

The Privacy Act calls for certain activities when a federal agency creates or modifies a system of records (including elimination of records). It is important to recognize that a system of records may be paper based as well as electronic. When the agency collects and stores PII in records and the PII is actually retrieved by a personal identifier, the agency is required to establish the statutory need for the collection, disclose the collection, describe its contents and declare the routine uses for that agency or any other agency that will use the information. This disclosure, a SORN, must be made to OMB and Congress and must be published in the Federal Register in advance of the system becoming operational and when any new routine use (including any new data element that the agency will maintain, retrieve, and use) is adopted by an agency. The OMB has also directed agencies to make links to their current SORNs available from their websites. This requirement applies equally to pilot or test systems that are using actual “live” PII; the Privacy Act does not specify any exemptions for such systems.

SORNs are the principal way the Privacy Act implements the prohibition against secret systems in the 1973 Code of Fair Information Practices. SORNs amount to a public paper trail of all government “systems of records”. Nongovernmental organizations (NGOs) play an important role in this process. Unlike the vast majority of the American public, privacy advocacy NGOs review the SORNs and other relevant notifications published in the Federal Register. When they find something they consider problematic, they readily voice their concerns.
The specific items in the SORN include:

- Name and location of the system
- Categories of individuals whose PII is collected
- Each routine use
- Authority for maintenance of the system
- Policies for storage, retrieval, access control, retention and disposal of records
- Title and business address of the responsible agency official
- Agency procedures for an individual to inquire if a system contains records about the individual
- Agency procedures for an individual to gain access to records about the individual
- Categories of sources of records
- Disclosures to consumer reporting agencies and whether the system is exempt from access by the individual

### Critical Aspects of a SORN

- Acts as legal notice to the public
- Must specify routine uses
- Must be revised and republished if a new routine use is created
- Prior to system operation, must be provided to OMB and Congress and published in the Federal Register
- Required for pilot or test systems using real PII

### 1.4 Privacy Act Statement

In addition to SORNs, agencies must provide a separate statement (notice) to individuals when collecting Privacy Act information from them. This statement must be included on the form used to collect the information from the individual or on a separate form that can be retained by the individual. Although not required by the Privacy Act, prior OMB clearance may be required in some cases under the Paperwork Reduction Act to review the agency’s estimate of the paperwork burden imposed by the form. The Privacy Act statement must include the following items:

- The statute or other legal authority for soliciting the information
- The principal purpose(s) for which the information is intended to be used
- The routine uses to be made of the information (see the relevant SORNs)
• Whether the information is mandatory or voluntary, and the consequences not providing the information

Although this requirement applies to forms, the OMB recommends that such a statement also be given when collecting information orally from individuals. The OMB also notes that the act does not explicitly require such a statement when collecting information from a third-party source, but where feasible, the agency should inform the source about the purpose for which the information will be used and assure the third party that his or her identity will not be revealed to the subject individual (i.e., if such confidentiality is afforded by a Privacy Act exemption applicable to the relevant systems of records).9

1.5 Records Maintenance and Retention
Privacy Act records maintenance and retention requirements apply whether the records are maintained by the agency itself or by contractor personnel.10 The retention requirements must be stated in the agency’s SORN; the records are considered to be maintained by that agency, and subject to the agency’s SORN, even when the records have been transferred temporarily for storage, processing or servicing to NARA.11

NARA retention schedules (discussed in more detail in Chapter 7) provide the basis for the records retention periods stated in the SORN. In an ideal world, the NARA and SORN retention periods would always be identical. As a practical matter, NARA’s primary concern is preventing premature disposal of records, but sometimes the retention period specified in a SORN exceeds the period that is specified by the NARA schedule. Over-retention can have obvious privacy implications and poses long-term storage issues that are contrary to an efficient and effective records management program. In these cases, an explanation for the extended retention period should be provided in the SORN. Conversely, SORNs should not specify a retention period shorter than legally required under the applicable NARA retention schedule(s).

1.6 Agency Use of Data and Exceptions
Agency use of PII under the Privacy Act is bound by 12 exceptions. Without these exceptions, an agency would have to obtain the consent of individuals each time it intends to use or disclose their records. The breadth of the exceptions has rendered this process very infrequent.12

The 12 use exceptions to the Privacy Act are:13

• Performance of regular duties by an agency employee (need-to-know basis)
• FOIA disclosures
• Routine uses as specified in the applicable SORN
• Census Bureau or survey functions
The Privacy Act and the E-Government Act

- Statistical research if not individually identifiable
- Disclosure to the National Archives
- Law enforcement requests
- Compelling health or safety circumstances
- Congressional committee with appropriate jurisdiction
- Government Accountability Office (GAO) duties
- Court order
- Consumer reporting agencies

The most utilized of these Privacy Act data use exceptions are:
- Performance of agency duties
- Routine use
- Law enforcement
- Court order

1.6.1 Agency Utilization of Routine Use

Exemptions 1 (intra-agency use on a need-to-know basis) and 3 (published routine uses) form the backbone of day-to-day Privacy Act practice within federal agencies. Over time, however, routine uses have come to be written very broadly. Some commentators believe this has been merely for expediency, to avoid having to publish a revised SORN in the Federal Register if a use is modified. Others believe that the objective has been to limit the public’s ability to know how PII is being processed, used and shared within agencies. Still others believe that agencies, as a practical matter, write broad routine uses to give themselves the widest flexibility in using and disclosing PII protected by the act. Whatever the reason, very broad routine uses can seriously undermine the purpose specification under FIPs. Privacy professionals in the federal government should carefully assess whether the routine uses, as written, provide sufficient information to the public about the protection of PII and should be prepared to challenge those within their organizations who wish to adopt broad routine use language that may circumvent the intent of the Privacy Act.

1.7 Individual Access, Agency Procedures, Exempt Systems and Right to Court Review

With certain exceptions, an individual has significant access and disclosure rights under the Privacy Act. These rights include the right to access data about the individual kept by federal agencies and the right to file civil claims if the agency has breached the Privacy Act’s requirements. Some records may not be kept under any circumstance unless specifically allowed by statute, such as any record regarding the exercise of an
individual’s First Amendment rights. In addition, the act allows agencies to exempt certain record systems from access by the individual and various other provisions of the act if such exemptions are published as an agency regulation in the Federal Register (e.g., Central Intelligence Agency and other classified systems, criminal law enforcement agency systems and personnel or contractor security investigation systems that would reveal a confidential source).14

1.7.1 Access and Correction

Certain rights to access, copy and request amendment of records are granted to the individual.15 Once a request is made, the agency is required to acknowledge receipt of the request within 10 working days. It must promptly make corrections or inform the individual of the refusal to amend, the reason for the refusal, the procedures for review of the refusal and the name of the agency official to contact to dispute the refusal. The agency must allow a request for review of the refusal and process that request within 30 working days, unless the agency extends the review for good cause. If the agency has refused the individual’s request, the individual is permitted to file a statement of disagreement with the agency. The agency is also required to inform people and agencies to whom the record is subsequently disclosed of any disputed portion of the record, together with a copy of the individual’s statement and any optional statement by the agency of the reasons it refused to make the requested amendment. The agency must also inform persons or agencies to whom it previously disclosed the record of any correction or notation of dispute, except where the agency was not required to account for the prior disclosure (i.e., intra-agency disclosures and FOIA). In the event of an agency’s refusal of the individual’s request to amend, the individual is ultimately allowed judicial review.

1.7.2 Agency Procedures

The Privacy Act requires agencies to establish procedures implementing its provisions.16 These include procedures for access requests, establishing the identity of a person making a request and appeal of a denied access request.

1.7.3 Civil and Criminal Penalties

After exhausting the agency procedures outlined above, an individual can file suit in U.S. federal court in the following cases: a) the individual has had a request to amend a record refused by an agency; b) an agency refuses a request for access to records; or c) the agency fails to comply with the data quality safeguards identified above, or any other rights established under the act. Without deference to any agency determination or review, the court shall review the matter and may amend the individual’s record, take whatever other action it deems appropriate and/or grant attorney fees, and in some cases, litigation costs against the agency.

In cases of refusal to amend a record or to comply with an access request, the court may require amendment of or access to the record, and may assess attorney fees and
other “reasonably incurred” litigation costs. (The court may also privately examine the contents of the record to determine whether any exemption applies and access may be properly denied.) In lawsuits where the court determines that the agency intentionally or willfully failed to maintain records properly under the act, or to comply with any other provision of the act, the agency can be liable for actual damages sustained by the individual, but not less than $1000, plus attorney fees.17 Such civil cases must be brought within two years of the date on which the cause of action arises or, if the agency materially and willfully misrepresented material information, within two years of discovery of the misrepresentation.

The act also provides for criminal penalties against agency officers or employees who have possession of, or access to, Privacy Act records for willfully disclosing them in violation of the act, and against such officers or employees for willful maintenance of an unpublished system of records. The act also deems it a crime for any person to obtain Privacy Act records knowingly and willfully from an agency under false pretenses.18

1.8 Computer-Matching Provisions
The Privacy Act was amended by the Computer Matching and Privacy Protection Act of 1988. The provisions under this amendment, as further amended in 1990, require federal agencies that use computerized means to match data between electronic federal Privacy Act record systems, or to match data from any such federal system with nonfederal records in connection with granting or recouping financial benefits (or for personnel or payroll purposes) to publicly disclose the matching in a written agreement between the agencies. The written agreement explains the scope and purpose of the matching and must include procedures and safeguards to protect individual privacy.

There are three important aspects of the computer-matching process:

- Generally does not apply to intra-agency matching
- Requires matching agreements overseen by agency data integrity boards (DIBs)
- Matching agreements must be made available to Congress and the public

1.8.1 Components of the Matching Program
The Privacy Act describes the major elements required for matching programs.19 As noted above, there must be a written data-matching agreement between the agencies, specifying the purpose, justification and legal authority for the matching program, including a description of the records to be matched and procedures for notifying affected individuals that they may be subject to verification through matching programs.

The written agreement must also establish procedures for:
- Verifying the information produced by the matching program
- Retaining and destroying the information
- Providing administrative, technical and physical security of the matched records
- Prohibiting duplication and further disclosure unless required by law
- Allowing use by a recipient agency, including return and disclosure
- Assessing the
accuracy of records. The GAO is granted access to the records to verify compliance with the matching agreement. Agencies may not operate a matching program until they provide a copy of the matching agreement to House and Senate oversight committees at least 30 days before the program begins. Matching agreements must also be made available to the public upon request. The agreement is only allowed to be in effect while the agency’s DIB agrees, and not longer than 18 months, unless the agency DIB certifies the need to extend the agreement for an additional 12 months.

1.8.2 Rules Before Benefits Are Denied

Agencies must comply with certain requirements to ensure individual administrative due process before the matched data is used to suspend, reduce or deny a federal financial benefit or payment. Agencies must independently verify the information, unless, following OMB guidelines, the DIB determines that the information used is accurate to a “high degree of confidence” and is limited to confirming the individual’s identity and amount of benefits paid to him or her. An individual must receive a notice of the findings and be given an opportunity to contest the findings until the expiration of a time period established by the agency or by statute, or within 30 days if another time period has not been established. In the absence of a DIB determination, the agency’s independent verification requires investigation and confirmation of the specific information used as a basis for the adverse action. This information includes, where applicable, the amount of an asset or income and the period that the individual had the asset or income. The data-matching provisions have an exception allowing an agency to take any appropriate action for public health or safety reasons without waiting for the notice period to expire.

No agency may disclose records to another agency for matching purposes if the source agency believes the matching agreement or the procedures for individuals to contest the match are not being followed by the recipient agency. Furthermore, no agency can renew a matching agreement unless the recipient agency certifies that it has complied with the agreement and the source agency has “no reason to believe” that the certification is inaccurate. Any new or significantly changed matching program must be reported in advance to appropriate House and Senate oversight committees and the OMB.

1.8.3 Creation and Use of the Data Integrity Board

The matching provisions of the Privacy Act require that each agency participating in a matching program create a DIB composed of senior officials and the agency’s inspector general. The DIB shall:

- Review, approve and maintain all matching agreements
- Review all existing matching programs annually to determine compliance with laws, regulations, guidelines and agreements, and assess the cost and benefits of the agreements
The Privacy Act and the E-Government Act

- Review the continued justification for each matching program annually
- Compile annual reports on matching programs for the agency head, OMB and public requests
- Serve as the matching program’s information clearinghouse for accuracy, reliability and completeness of records used for data matching
- Provide interpretation and guide agency compliance
- Review agency matching programs’ record-keeping and disposal policies
- Report, in its discretion, on other agency matching activities that are not under agreement

The DIB shall, with certain exceptions, require a cost-benefit analysis before approving any matching program. Disapproval of a matching agreement by the DIB may be appealed to OMB, which can override the disapproval. If both the DIB and the OMB disapprove a matching program proposed by the agency’s inspector general, he or she may report the disapproval to the agency head and Congress.

1.9 The OMB’s Role and Other Privacy Act Responsibilities

Under the Privacy Act, the OMB is charged with the responsibility to supervise agencies’ implementation of the act’s provisions. In order to perform this task, the act provides that the director of the OMB shall develop and prescribe guidelines and regulations, as well as provide assistance and oversight of their implementation by agencies.22 (Although not explicitly prescribed within the act, additional legal guidance has been provided to federal agencies by the Department of Justice, Office of Privacy and Civil Liberties.) The Department of Justice asserts that its overview was not created to offer policy guidance—that is the OMB’s responsibility—but that it is intended to legally analyze and refer to court decisions regarding the act’s provisions.23

In the case of the OMB’s policy guidance, the main directive is OMB Circular A-130 and its Appendix I, “Federal Agency Responsibilities for Maintaining Records About Individuals.” The appendix identifies relevant responsibilities of the heads of agencies, including review of contracts, record-keeping practices, violations of the Privacy Act, personnel training, and SORNs. The appendix also identifies agency reporting requirements, and sets forth specific requirements for the Department of Commerce, Department of Defense, Office of Personnel Management, NARA, and the OMB itself. This OMB circular is discussed further in Chapter 6.

The OMB issued its original Privacy Act guidelines in the Federal Register in July of 1975, laying out responsibilities for Federal Agencies under the Act.24 In order to update these guidelines, it issued supplemental guidance in December of the same year, and again in May of 1985.25 In addition to this guidance, the OMB has issued provisions on the implications and relationships between the Privacy Act and other legislation,
such as the Debt Collection Act of 1982\textsuperscript{26} and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996.\textsuperscript{27} The OMB has continued to supplement its guidance over time with other issuances, including computer-matching guidance and other technical guidelines to carry out the requirements of the Privacy Act as well as the E-Government Act, which is discussed later in this chapter.\textsuperscript{28}

1.10 Miscellaneous Provisions of the Act

In addition to the responsibilities discussed above, the act sets forth certain miscellaneous provisions designed to ensure that the privacy and civil liberties of individuals are protected. For example, subsection (n) of the act prohibits the unauthorized sale or renting of individual names and addresses. Section 7 of the act further prohibits any federal, state or local government agency from denying any individual any right, benefit or privilege provided by law based on an individual’s refusal to disclose his or her SSN.

1.10.1 The Relationship Between the Privacy Act and FOIA

Although FOIA and the Privacy Act seem to have the opposite goals of ensuring access to records (FOIA) and preventing disclosure of records (Privacy Act), they are similar in their provisions for procedural rights to request records and receive a response.\textsuperscript{29} The statutes work together to ensure access to agency records while protecting the privacy rights of individuals. The Privacy Act provides only U.S. citizens and lawful permanent residents right of access to their own records, whereas FOIA provides a general right of access to agency records for any requester (e.g., non-citizens, non-permanent residents, businesses) seeking access to such records. Privacy Act exemptions to access apply to entire systems of records, whereas FOIA exemptions apply to particular records and parts of particular records.

While FOIA allows agencies to withhold records that would constitute an unwarranted invasion of privacy from disclosure to persons or entities other than the individual, the Privacy Act often requires access to the same records by the person to whom the records pertain. Conversely, records that are part of systems exempted from certain provisions of the Privacy Act related to the subject individual are not necessarily exempt from disclosure to third parties under FOIA. To disclose a Privacy Act record under FOIA to a third party, however, the agency must receive a formal FOIA request and determine that the agency cannot withhold the record on grounds that it would constitute an unwarranted invasion of the subject individual’s privacy. The Privacy Act does not permit discretionary disclosures (without a FOIA request) outside of the use exceptions discussed earlier. For first-party access requests from the subject individual, the agency must consider the exempt status of the requested record under both the Privacy Act and FOIA. Thus, the requested record must not only be part of an exempt system of records under the Privacy Act (see above) but must also be exempt from disclosure to the individual (on other non-privacy grounds) under the FOIA to bar an individual’s access following that statute as well.