



The Privacy Act, an Employee Guide to Privacy

March 1, 2016

Office of the General Counsel

GENERAL PROVISIONS

While the Freedom of Information Act opens the business of Government to the public scrutiny, the Privacy Act establishes safeguards for the protection of records the Government collects and keeps on individuals. Additional information regarding the Freedom of Information Act and how it relates to your job is available in DCAA Guide: The Freedom of Information Act, A Manager's Guide to a Complex Law.

The Privacy Act provides the Government with a framework in which to conduct its day-to-day business when that business requires the collection or use of information about individuals. Specifically, it requires that the Government:

- Maintain no secret files on individuals;
- Inform individuals at the time it is collecting information about them, why this information is needed, and how it will be used;
- Assure that personal information is used only for the reasons given, or seek the person's permission when another purpose for its use is considered necessary or desirable;
- Allow individuals to see the records kept on them; and provide individuals with the opportunity to correct inaccuracies in their records.

The Privacy Act binds Federal agencies to a "code of fair information practices." The code sets standards which each Federal agency must meet as it collects, maintains, and uses information. As an employee who works with Federal records, you see effects of these standards.

For example, the last Government form for personal information you were asked to complete should have contained a Privacy Act Statement that indicated the authority for collecting this information, why the information is needed, who would use the information, and what the consequences would be for not providing the information.

Other examples of fair information practices point out the role of Federal agencies as stewards, rather than owners, of information they possess. Although Federal agencies have control over information, the code of fair information practices clearly establishes that these agencies are not free to collect, use, and disclose information as they please. The responsibility of stewardship requires care and fairness in the way information is collected and held, a concern that those who have rights to this information will be given access to it, and vigilance to protect the information from those who have no legitimate use for it.

RECORDS COVERED BY THE PRIVACY ACT

The Privacy Act applies to Federal agencies. Federal agencies are defined in the law as all agencies, offices and departments of the Executive Branch, independent regulatory agencies such as the Securities and Exchange Commission, and Government-controlled corporations such as the Postal Service.

The Privacy Act does not apply to records held by the Legislative and Judicial Branches of the Federal Government, state and local governments or private organizations, except in isolated instances where these organizations hold special types of contracts with a Federal agency.

Specifically, the Privacy Act applies to Agency records that:

- Contain information on individuals; and
- Are filed so that the records are retrieved by use of the person's name or some other personal identifier such as a social security number.

The Privacy Act defines an individual as a U.S. citizen or alien lawfully admitted for permanent residence. Excluded, then, from Privacy Act coverage are the records that Federal agencies maintain on organizations and businesses, including small businesses, even where the company's trade name could be the same as that of the owner. Also excluded are records that Federal agencies may maintain on deceased persons.

Privacy legislation had its origins in the late 1960's when people became concerned about abuses that could occur with computer data banks. The Privacy Act applies to personal information stored on computers as well as in manual files. Easy access to and quick transfer of information are features that make the computer a valuable tool. However, these very same features make the confidentiality of information difficult to protect. Since the Privacy Act became law, the Federal Government has been developing and establishing safeguards for the protection of personal information held in computer data banks.

DCAA RECORDS

DCAA has published in the Federal Register a description of its record systems that are covered by the Privacy Act. Included among these are personnel, security, and other administrative files. In addition, the Office of Personnel Management and other Federal agencies have also published notices of record systems that may be of interest to you, such as official personnel folders, discrimination complaint records, and other personnel-related records.

For each one of these record systems, a specified person, known as a system manager, is responsible for answering questions you may have about seeing your records, and amending or correcting information contained in them. This person, along with his or her mailing address, is listed in the Federal Register notice. Summary information about all record system notices in the Federal Government is published in the Federal Register bi-annually and is periodically updated. A complete listing of DCAA and applicable Federal Government System Notices are contained on the DCAA web site.

RIGHTS AND RESPONSIBILITIES OF DCAA EMPLOYEES

As a DCAA employee you "wear two hats," one as a citizen entitled to the full protection and rights established by the Privacy Act, and the other as a Federal employee working with records containing personal information and sharing some responsibility in carrying out the

requirements of the law. The seriousness of this responsibility is evident from the penalties the Privacy Act imposes upon Federal employees who willfully violate key sections of the law. Fines up to \$5,000 can be imposed for willfully disclosing personal information that should not be released under the Privacy Act, or for maintaining secret records on individuals.

The following presents a summary of your rights and responsibilities under the Privacy Act.

COLLECTION OF PERSONAL INFORMATION

RIGHTS

Whenever you are requested to provide personal information to a Federal agency, you are entitled to know: the legal authority for requesting the information; the purpose for collecting it; what routine uses (disclosures) might be made of this mandatory or voluntary disclosure; and what effect your refusal to provide the information would have.

RESPONSIBILITIES

You must collect only personal information that is relevant and necessary, not simply useful, to accomplish a specific objective. Whenever you request personal information from someone, you must inform him or her in writing of the legal authority for requesting the information, the purpose for collecting it, what routine uses will be made of this information, whether a response is mandatory or voluntary, and what will be the effect if he or she refuses to respond. Also, whenever you ask a person for his or her social security number, you must state the legal authority and purpose for requesting it, and whether a response is mandatory or voluntary. You should always attempt to collect personal information directly from the individual rather than from other sources wherever practicable.

ACCESS TO RECORDS

RIGHTS

You can request to see your records in writing, in person, or by telephone. You should describe the information you wish to see. Blanket requests for "all the information the agency has on me" cannot be honored. If you appear in person, identification will be required to verify you are the person whose record you are requesting.

If you have no suitable identification, you will be asked to certify your identity in writing.

Another person of your choice may accompany you when you check your records.

You are entitled to receive a copy of your record or an acknowledgment of your request within a reasonable period.

You are not required to give a reason for your request; however, the more specific your request, the faster you can expect a response.

RESPONSIBILITIES

When someone requests to see his or her record, you must verify the identity (a driver's license, passport, alien or voter registration card) or require the person to certify in writing that he or she is the subject of the record requested and that the person understands that any knowing and willful request for a record under false pretense is a criminal offense subject to a \$5,000 fine. If the request is by telephone, you should verify the person's identity, if possible, or require that a request be made in writing.

You must have the requester of a record authorize in writing the presence of another person if he or she desires someone to be present for the inspection and discussion of the record.

When a request for a record is received, you should check to see whether a record on the person exists in a system of records that is subject to the Privacy Act. The system manager or another designated official must either present the record or a copy of it, or acknowledge the request within ten working days or as soon as possible.

You should not ask the person to give a reason or justify a need to see his or her own record.

ACCESS TO MEDICAL RECORDS

RIGHTS

Special rules apply to medical records. In most cases, when you request your medical record, you will be able to see it directly. However, when it appears that the medical information could have an "adverse effect" on you, the record will be sent to a representative you name, such as your family doctor or other responsible individual, who would be willing to review the record and inform you of its contents.

RESPONSIBILITIES

For certain medical records, you must require the requester to designate a representative, such as a family doctor, health professional, or other responsible individual who would be willing to review the record and inform the requester of its contents. Because of the sensitive nature of medical records, you may also require additional identification from the requester, such as a notarized statement.

AMENDMENT OF RECORDS

RIGHTS

If you wish to correct, delete or add information, you must identify the record and give reasons for the desired change. In general, only factual, verifiable information is subject to amendment under the Privacy Act.

You must verify your identity as described earlier.

If your request for amendment is accepted, then the information in your record will be changed and you will be informed of this action.

If your request to amend your record is denied, the agency must tell you the reasons for this decision and how you can appeal it.

If you choose to appeal the denial of your request, a review must be made within 30 days unless you are notified of a delay for good cause.

If your appeal is upheld, your record will be amended as requested.

If your appeal is denied, the official who reviewed your case must tell you the reasons and inform you of your right to file a statement of disagreement with your record and your right to seek judicial review of the decision.

RESPONSIBILITIES

According to established procedures, as outlined in DCAAR 5410.10, DCAA Privacy Act Program, you must acknowledge a request to amend a record within 10 working days and advise the person when he or she can expect a decision on the request. A review should normally be completed within 30 days.

You must receive verification of the person's identity and advise the person when he or she can expect a decision on the request. Remember the review should normally be completed within 30 days.

If a person's request for amendment is accepted, you must correct the record as well as notify all organizations or persons who have received copies of the record of the amendment that has been made. The only exception would be if the request were under the FOIA or within DCAA.

If a request for amendment is denied, you or a designated official must inform the person of the decision and the procedure for appealing it, as established in DCAAR 5410.10, DCAA Privacy Act Program.

Within 30 days, the official reviewing the appeal must inform the person whether his or her appeal is upheld or denied or explain good cause for a delayed decision.

If the person's appeal is upheld, you must correct the record and notify all organizations or persons who have received copies of the record of the amendment that has been made except under the FOIA or within DCAA.

If the appeal is denied and the person files a statement of disagreement, you or a responsible official must send this statement to everyone who has received a copy of the record

(except under FOIA or within DCAA), as well as to everyone who will receive the record in the future.

SUMMARY

If the Privacy Act is to achieve its objectives, there must be cooperation by every Federal employee who works with records containing personal information. You are more than a program analyst, personnel management specialist, administrative assistant, computer programmer, auditor, and so on. In the course of your work you become a steward or custodian of the information entrusted to you. In order to meet the responsibilities of this stewardship, there are certain steps you should take:

1. Learn as much as possible about the requirements of the Privacy Act and how these requirements relate to your job. This can be accomplished through formal training, on-the-job training, discussions with your supervisor, and reading to keep up with new developments, policy guidelines and operating procedures. Acquaint yourself with DCAAR 5410.10, DCAA Privacy Act Program, which contains Privacy Act policies and procedures.
2. Consider how you handle the information you work with, and what measures, if any, you need to take to safeguard the personal information in your possession.
3. Become familiar with the kind of information that is available under the Privacy Act. Certain employees within DCAA components have been designated to provide assistance in meeting the requirements of this law. These individuals are "Privacy Act Coordinators" for their respective regions.
4. Respond promptly to requests for information by quickly referring such requests to the responsible official.
5. Take care that personal information is not disclosed to someone unless that individual, such as another Federal employee, requires the information in the performance of his or her job, or that individual has received prior permission to see the information from the subject of the record, or disclosures of the record are authorized by law.

In conclusion, it should be noted that this pamphlet has only tried to touch on the main points concerning your rights and responsibilities as a Federal employee under the Privacy Act. You are urged to become more familiar with DCAA's policies on the Privacy Act and to consult your supervisor whenever you have any questions.