Privacy: The Small and Large of It
Anna W. Nusbaum, CRM
Manager, Sandia National Laboratories

Introduction:

The topic of Privacy is complex, multi-faceted, and often emotionally laden. This paper will cover the following topics, in an effort to further understanding of federal regulations and activities, the balancing act that necessarily occurs in business, and what role a records manager can play.

- Definitions
- The Privacy Act
- “Private” companies
- Potential areas of concern
- Expectations
- Corporate responsibilities
- Case studies
- Records Manager’s role

Definitions

Privacy:

Privacy is a noun that stands for the quality or condition of being secluded from the presence or view of others. It is the state of being free from unsanctioned intrusion. An individual would maintain her privacy by not sharing particular personal information about her. A Company maintains the privacy of its employees by exercising certain protection measures concerning access to personal information.

Private:

Private is an adjective that describes a noun as being secluded from the site, presence or intrusion of others. It can also mean that something is designed or intended for one’s exclusive use or that something is of or confined to the individual; that it’s personal or not available for public use, control, or participation. Something is private when it belongs to a particular person or persons, as opposed to the public or the government. When you keep a secret, you are keeping certain information private. You expect a company to keep certain information about you as private, so that it is not disclosed to others.

The Privacy Act

The Privacy Act can generally be characterized as an omnibus “code of fair information practices” which attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies. The historical context of the Act is important to an understanding of its remedial purposes: In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal; it was also concerned with potential abuses presented by the government’s increasing use of computers to store and retrieve personal data by means of a universal identifier -- such as an individual’s social security number.

The Privacy Act

The Privacy Act governs the information collection behavior of federal agencies. The purpose of the Privacy Act is to balance the United States Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from United States Federal Agencies' collection, maintenance, use, and disclosure of personal information about them.
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.
The Act focuses on four basic policy objectives:
1. to restrict disclosure of personally identifiable records maintained by agencies;
2. to grant individuals increased rights of access to agency records maintained on themselves;
3. to grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete;
4. to establish a code of “fair information practices” which require agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Agencies must tell people why it is collecting personal information and that is done through announcements in the Federal Register. Additionally, forms used to collect that kind of information must have the Privacy Act statement on them.

A system of records, in the Privacy Act world, is 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.

A record, in the Privacy Act world, is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains his/her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

No agency shall disclose any record in a Privacy Act system to anyone without prior written consent of the individual. There are, of course, some exceptions. Eleven of the exceptions are permissive, including need to know in performance of duties; routine uses of the system; census reporting; statistical research; National Archives; law enforcement; health or safety of an individual; Congress; General Accounting Office; court order; debt collection. One exemption is required: release under FOIA.

The Privacy Act gives an individual the right to
1. see and copy files that the federal government maintains on him or her;
2. find out who else has had access to the information;
3. and request a change in any factual information that is not accurate or relevant. (Opinions are protected information under the Privacy Act.)

Every agency and contractor supporting an agency in its Privacy Act obligations is expected to designate a Privacy Act Administrator. It is the responsibility of the Privacy Act Administrator to:
1. Coordinate compliance with the Privacy Act of 1974 with respect to the systems of records in use;
2. Monitor third party requests for access that are not for routine uses of the records as provided by the Privacy Act Coordinators; and
3. Hold periodic meetings with Privacy Act Coordinators to assure that the Privacy Act provisions are administered effectively and uniformly.

The Privacy Act of 1974 also applies to contractors who maintain certain records for United States Government agencies. These records are identified as a Privacy Act system of records in the contracting document. When a contractor performs a record-keeping function for a government agency, and the system of records is identified in the contractor's contract with the government agency as a system of records subject to the Privacy Act, then the contractor and its employees become subject to the Act with respect to those systems of records. For example, twelve systems of records are maintained by Sandia for the Department of Energy that are subject to the provisions of the Privacy Act of 1974.

“Private” Companies
The issue of privacy is not solely the concern of federal agencies and its contractors being compliant with the Privacy Act. Private companies also must address concerns regarding employee privacy and the privacy of information collected about their customers. I'll discuss some cases later in this report that will highlight this.

Every state in the United States has some kind of privacy, personal information protection, or non-disclosure regulation. In California, it is the Financial Privacy Law. In Massachusetts, it's the Declaration of rights. In New Mexico, it is the Individual Right to Privacy law. This admittedly makes it quite challenging for a company that operates in more than one state to be confident of compliance with each state's regulations.

As mentioned in the Privacy Act discussion, companies, by virtue of working under a contract to a federal agency, may also have Privacy Act obligations, to the extent required under their contract with the federal agency.

Areas of Concern

“The erosion of privacy that has occurred in this century is in part due to the fact that privacy is an individual's interest, while intruding on privacy is in the interest of an institution, whether it be governmental or private. When these two interests collide, and an ad hoc balancing is conducted, it she be no surprise that, given the absence of defined legal rights, the institution (whether it be the police, a prosecutor, bank, insurer or direct marketer) usually wins out.” (page 5, Privacy Times, September 30, 1998)

E-mail, a pervasive recorded information tool, presents complicated privacy issues. The increase in commerce on the Internet and the ease with which personal information can be collected and lost, collected and abused, presents some conflicting presentations of rights. Our own personnel and medical files are not always maintained as privately as we would wish. Collection of information into personnel and medical files is best limited to the immediate purpose of collection; companies need to avoid the “might as well as” syndrome to collect more information that is required or needed. Companies, whether they are our employers or our service providers, will have conflicting drivers in the collection and then release of information about us.

“Just look at the Social Security number. In establishing a social security system, the U.S. Government understood that concern about a national identifier could threaten implementation of the new program, so it set the policy that the Social Security cards were not to be used for identification. Years later, when some State motor vehicle departments saw the SSN was a convenient number for driver’s licenses. Congress quietly authorized its use. Then it became the identifier for all government agencies. Then Congress required that you give it to your bank for tax purposes. Now the U.S. Transportation Department proposes to require it on all drivers’ licenses. Meanwhile, one of the information age’s fastest-growing crimes is identity theft, which begins with the theft of an individual’s SSN and is facilitated by institutions’ reliance on it.” Ibid.

Expectations

Employee Expectations

Increasingly, companies are making it more and more clear that company resources are for the conduct of company business. Therefore, an employee should not expect any privacy in the use of such company resources as computer workstations, e-mail applications, or his/her voice mail.

Twenty percent of companies with e-mail services regularly monitored e-mail in 1998, up from fifteen percent in 1997, according to the American Management Association. Sales of monitoring software quadrupled last year at one software company. Why the increase in monitoring? A recent string of legal cases has underscored e-mail’s power as a key prosecution weapon. Attorneys are calling e-mail the smoking gun of the 90s.

An employee can reasonably expect the company to have policies on employee and corporate responsibilities on protection of personal information. Various companies are using a multi-faceted approach with policies, an ethics
program, and education. A Company will likely not hand out a private phone number to anyone who asks, but it is reasonable to give the phone number to the employee's manager, for emergency use. In the best of cases, the amount of protection a company can provide to personal information is limited.

An employee can also expect reasonable access to his or her own records and an opportunity to clarify misleading information or to correct wrong information.

Customer Expectations

A company that wants to survive and even thrive does so with a variety of strategies, including "knowing the customer". Understanding what its current and potential customers want and value is essential to offering products and services that will sell. Collecting information about current customer preferences and demographic information about potential customers is not an invention of the Internet. The Internet makes it easier, however, to collect more information than was previously available or accessible.

Such information used to be jealously guarded as proprietary information; now companies must grapple with the ethics or propriety of sharing or selling that information to others. For example, is there any harm in selling a mailing list composed of a company's customers? What if the mailing list also contained the customers' purchases for the past year? Remember those warranty cards you fill in when you buy a new appliance? Ever wonder what the company did with that extra information they collect, such as whether you own a pet, what kind of soap you purchase, on the warranty card you completed for your recent toaster purchase?

The United States Federal Government plays a rather contradictory set of roles in the privacy of information arena. One role is that of protector of the national infrastructure, with the responsibility of making sure that telecommunication systems, transportation systems and other interstate systems continue to work. Another role is that of finding ways to efficiently deliver services we have come to rely on in an increasingly mobile population.

The Health and Human Services Department was tasked last year to create a health care identification numbering system. This Unique Health Identifier number would let the government, health insurers, hospitals, doctors and health researchers track peoples' medical histories from birth to death. Separation and dispersal of different information collections are a means of protection; however, when dealing with one individual, it is not the most efficient way to manage that individual's health care. But opposition to the system, from privacy advocates who fear the numbers could fall into the wrong hands or be used inappropriately by healthy providers and insurance companies, led HHS to hold public hearings around the country. The administration subsequently backed off on this proposal.

Corporate Responsibilities

Any company, to protect itself and to have well-informed employees, must have established and socialized policies on:

- The use of Corporate resources (whether the resources are only for the execution of work, or when may the resources be used for incidental personal use)
- What personal information is considered routine (specify what personal information will be routinely dispensed, what personal information is more closely protected and requires some formal request for release)
- What is the composition of personal information files (describe specifically what are the standard contents of personnel files, medical files, etc.)

Then, the company must support the policies with specific procedures and training, with expectations (and consequences) that the policies and procedures are consistently followed, and that any exceptions are unusual and well documented.

The policies and procedures must support protection and release of information regardless of format. Access protections must be logically consistent for both physical files and electronic files and databases.
Case Studies

International Commerce

There is conflict between the U.S. and the European Union in the protection of personal data. The EU directive is meant to facilitate the flow of information among EU member states, but its provisions threaten to cut off data exchanges with the United States. That is because Article 25 of the directive prohibits the release of personal data to third countries in the absence of adequate protection measures.

Europe’s privacy debate is influenced by historical tragedy: the Nazis storming into towns and grabbing lists of Jews, Communists, and other enemies so they could round them up. That’s why privacy is seen there as a human right and is guarded by a comprehensive law.

David Aaron, undersecretary of commerce for international trade says “that the United States does have an adequate privacy protection regime. It is very different in structure and process than the European system. But it is nonetheless effective, and we believe it deserves respect and attention.” He added that the U.S. system was essentially self-regulatory, following the U.S. Department of Commerce Principles, detailed below, while the Europeans prefer to protect individual privacy rights through legal means.

However, there is growing consensus in the U.S. among experts, the public, Members of Congress, and Vice President Al Gore, that privacy protection must be improved. Gore, in August of last year, announced steps to create an Electronic Bill of Rights to protect citizen privacy in an increasingly electronic world. “We live in a nation where people can get access to your bank account and your medical records more easily than they can find out what movies you rent at the video store,” he said.

Department of Commerce Principles

Notice: An organization must inform individuals about
✓ what types of personal information it collects about them,
✓ how it collects that information,
✓ the purposes for which it collects such information,
✓ the types of organizations to which it discloses the information,
✓ and the choices and means the organization offers individuals for limiting its use and disclosure

Choice: An organization must give individuals the opportunity to choose (opt out choice) whether and how personal information they provide is used (where such use is unrelated to the use(s) for which they originally disclosed it).

Onward transfer: Individuals must be given the opportunity to choose whether and the manner in which a third party uses the personal information they provide (when such use is unrelated to the use(s) for which the individual originally disclosed it).

Security: Organizations creating, maintaining, using or disseminating records of personal information must take reasonable measures to assure its reliability for its intended use and must take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

Data Integrity: An organization must keep personal data relevant for the purposes for which it has been gathered only, consistent with the principles of notice and choice. To the extent necessary for those purposes, the data should be accurate, complete, and current.

Access: Individuals must have reasonable access to information about them derived from non-public records that an organization holds and be able to correct or amend that information where it is inaccurate.
Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the principles, recourse for individuals, and consequences for the organization when the principles are not followed.

Surveillance Software

Codex Data Systems said it developed DIRT (Data Interception by Remote Transmission) to help catch pedophiles and will only sell the product to police, military or other government agencies. What sets DIRT apart is that it operates like a so-called Trojan horse, that is, a bug that can be secretly planted on a user's computer. Once embedded, DIRT captures all keystrokes, and if the target machine is on-line, it secretly transmits the captured contents to a remotely located DIRT-Control Central for analysis. By monitoring keystrokes, DIRT defeated the encryption program Pretty Good Privacy in a matter of minutes, according to a Techweek article.

AT&T has developed software that weeds out offensive or junk incoming e-mail. The company is developing software to understand taboo e-mail phrases.

Information and Identity Theft

A new brand of thieves are breaking into confidential credit bureau files and then using the stolen information to buy luxury cars under assumed identities. One of the victims was Los Angeles, California, County Supervisor Yvonne Brathwaite Burke. Burke said the thief took her name from the newspaper and paid a Georgia jeweler to run a credit check on her to obtain more data. The man obtained a driver’s license in the name of her husband and went on a spending spree. The man was finally caught when he brought the BMW back to the dealership to have a trailer hitch installed -- to tow the four Waverunners he had purchased. Although like other victims, Burke was not responsible for the fraudulent purchases, she said she spent months trying to clear up her credit reports after the fraud.

Connecticut Attorney General has filed suit against a Fairfield-based information broker, NRS Information Systems, Inc. The broker allegedly bribed bank employees for customer financial data, used pretext calls, and pulled credit reports.

An organized crime group appears to be behind the misuse of more than 1,000 Visa debit cards, resulting in fraudulent purchases of nearly $1 million. According to the Washington Post, the thieves were able to exploit a security programming error at the Transportation federal credit union. The thieves apparently used sophisticated computer programs that analyze sample credit and debit card numbers and then generate ones that turn out to be valid about half the time.

Representatives of biometrics companies admit that people object to being fingerprinted, or scanned, and worry about unforeseen and unauthorized uses of the personal identification data. One director of a biometrics company points out that biometric techniques can be used to protect individual privacy as well as organizational or corporate information. Verifying people's identification protects them against identity theft.

Information (Un)Protection

A 20-year-old computer consultant discovered a potentially major hole in the widely used Netscape Navigator and Communicator software. By writing JavaScript programming language, the consultant was able to capture and copy data automatically from a personal computer's "cache", which reveals which web sites the user has visited. A cache can also show personal data the user gave while registering at a web site. The consultant said a high-traffic web cold exploit the Netscape flaw to learn what other web sites their visitors are going to, and that employers could use it to check up on workers.

Hundreds and perhaps thousands of credit card numbers, home addresses and phone numbers were exposed for months through a gaping security hole on many small Internet auction sites. Security experts said the problem was alarming because, unlike ore technically complicated software problems, this one left records exposed to anyone who happened to click on the right Web page listings. The hole was discovered by Mark Dodd, who runs a site called AuctionWatch. During an Internet check on his domain name, he came across an index to another auction site. By manipulating a simple URL (web address), he could get full access to administrative controls of several sites containing thousands of records. The problem was most common at small and medium-sized auction sites.
Microsoft is offering two free software programs on its Internet site to strip out an identifying number that could be used to trace the authorship of some electronic documents. Those numbers are part of a 32-digit identifier created by Windows 98 whenever customers register their software with Microsoft.

Personal Privacy

A 1996 presidential order calling for a national immunization network threatens the privacy of all those individuals whose information would be part of the database. Since there is no protection for the confidentiality of immunization records, privacy advocates fear such information could be linked, through social security numbers, to other employment and financial information. Such linking could lead to non-immunized or under-immunized individuals being denied medical coverage, driver’s licenses, employment, tax deductions, or other benefits.

The Florida Department of Law Enforcement figures it made too much sense not to try to collect DNA information on children to protect and identify children. Yet when the department offered three school districts an opportunity to give parents a free ID kit with their children’s DNA, only one district agreed. “It’s the Big Brother is watching syndrome,” said Bill Johnson, spokesman for the Brevard County School District, which turned down the program. “Everybody’s concerned that we are tracking people and that kind of thing.”

The IRS has discontinued including the Social Security Number on taxpayer’s preprinted address labels. Because of privacy concerns, the IRS decided to eliminate the SSN from this year’s labels. As a result, taxpayers will need to write in their SSN in the spaces provided at the top of Form 1040, 1040A, or 1040EZ. Married taxpayers will also need to write in their spouse’s SSN, even if filing separately.

The Social Security Administration had been testing an online PEBES (Personal Earnings and Benefit Estimate Statements) in 1997, but has pulled the plug on the project because of concerns that it was too simple to breach the system and gain access to personal information. SSA originally planned to make the online application available again by January of 1998, but postponed that until the revamped PEBES can be tested.

An administrative law judge at the Federal Trade Commission has riled that Trans Union “invades consumers’ privacy when it sells consumers’ credit histories to third party marketers without consumers’ knowledge or consent”. Credit bureaus can develop lists for credit card companies for solicitation purposes. However, under the Fair Credit Reporting Act, the lists cannot be compiled for other business purposes. The government and Trans Union are arguing over whether Performance Data, a subsidiary of Trans Union, used credit data to generate mailing lists for catalog houses and others. The company contends the lists did not rely on credit information.

In his syndicated column, Bill Gates responded to a question concerning the fundamental fairness of being able to use technology to find out all sorts of personal information about individuals. Citing a number of examples in which individuals voluntarily provide personal information to companies in return for some benefit, Gates noted that “information at your fingertips is likely to cause societies to revisit the question of what should be public and what shouldn’t. Ultimately it’s a political rather than a technological issue.”

The Records Manager’s Role

There is not a better-qualified individual to dig into and understand the legal, political, and regulatory issues about privacy than you, as a records manager. The attorneys look at the legal issues; other management is looking at the political issues, and likely no one else is paying much attention to the regulations. You can be the resource and consultant to your company in this issue.

Evaluate the existing policies and procedures, and involve others in the review, using the multi-discipline perspective. For example, in an e-mail policy, are employees informed about what the company’s expectations are regarding the use of its computer systems and e-mail applications. If a company chooses, the policy can put employees on notice that the employer monitors internal e-mail.

During your education and training sessions, you can:

> identify those records series in your retention schedule that can have potential privacy issues,
provide hints on how to safely and respectfully handle records and information that contain private information, and
show managers and staff how to balance the information needs of individuals and the information collectors.

In your position, you will be doing your HR department (and your medical department if you have one) a great service in helping them standardize the contents that belong in both the official corporate files for personnel and medical records, and in the managers' personnel files. Junk in personnel folders is a smoking gun!

Some Helpful Information Resources

Here are some very useful (albeit rather expensive) resources in pursuing your understanding of the issues and activities surrounding privacy:

*BNA Electronic Commerce & Law Report,* weekly, $868.00/year; The Bureau of National Affairs, Inc., 1231 25th St. NW, Washington, DC, 20037-1197

*ACCESS Reports – Freedom of Information,* bi-weekly, $325.00/year; Access Reports, Inc., 1624 Dogwood Lane, Lynchburg, VA 24503. E-mail: 75111.743@compuserve.com

*PRIVACY TIMES,* bi-weekly, $275.00/year; Privacy Times, PO Box 21501, Washington, DC 20099.