Some Privacy Issues

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (A. Westin)

A claim is not the same as a right.

A claim is defined as something that one party owes another. Someone may make a legal claim for money, or property, or for Social Security benefits. A claim also means an interest in, as in a possessory claim, or "right" to possession, or a claim of title to land.

A right is defined as an entitlement to something, whether to concepts like justice and due process, or to ownership of property or some interest in property, real or personal. Rights include various freedoms, protection against interference with enjoyment of life and property, civil rights enjoyed by citizens such as voting and access to the courts, natural rights accepted by civilized societies, human rights to protect people throughout the world from terror, torture, barbaric practices and deprivation of civil rights and profit from their labor, and such American constitutional guarantees as the right to freedoms of speech, press, religion, assembly and petition.

One way to see the difference is captured in this statement: A right is something you have- something you are entitled to; a claim is something you assert you should have- something you (must) state or affirm you ought to be able to have.

The following is a (partial) list of institutions which have collected and stored information about people in contemporary society.

1) Vital statistics (birth, social security number, marriage, death, etc.)
2) Education (school records- grades, activities, etc.)
3) Financial (bank records, stocks owned, mortgages, loans, insurance, etc.)
4) Medical (health records, immunizations, psychiatric reports, diseases, illnesses, etc.)
5) Credit (credit cards, debit cards, purchases, credit score, etc.)
6) City government (property ownership, property taxes, home improvements, repairs, etc.)
7) Employment (social security number,earnings, deductions, work record, work history, etc.)
8) Customs and immigration (passports, visas, travel itineraries, duties paid, etc.)
9) Police (arrests, convictions, warrants, bail settings and amounts, paroles, sentences, etc.)
10) Welfare (payments, history, dependents, etc.)
11) Stores (credit cards issued, credit record, purchases, etc.)
12) [Private] Organizations, (memberships, activities, etc.)
13) Military (service record, including deployments to active war zones, discharge status, etc.)
14) Motor vehicles (driver's licences, ownership, registration, accident record, insurance, etc.)
15) Internet activity (search terms used, sites visited, purchases made, etc.)
16) Social media (all of the above?, depending on which platform you are on, etc.)

Privacy “Bill of Rights” proposed in 1973 U.S. government report:

- There should be NO personal data record-keeping system which is kept secret from people whose information is collected by and stored in that system;
- There MUST be a procedure for individuals to find out what information about them is kept in a record and how that information is used;
- There MUST be a procedure through which individuals can prevent information collected about them for one purpose being used or made available for other purposes without their consent.
- There MUST be a procedure for individuals to correct or amend any record containing identifiable information about them;
- Any organization or institution that collects, creates, maintains, uses or disseminates records containing personal information about individuals MUST assure that the information is used for its intended purpose and MUST take precautions to see that the information is not misused.

These rights were intended to apply to government agencies/institutions in their data collection, sharing, and dissemination of personal information.
The formulation of this “Bill of Rights” was followed by the passage of the Privacy Act of 1974.

Privacy Act of 1974

This legislation applied to the agencies, departments, and offices of the ***federal government***. Its provisions:

1) Permit individuals to determine what records pertaining to them are collected, maintained, or disseminated by those agencies, departments, and offices;
2) Permit individuals to prevent records pertaining to them obtained by those agencies for one purpose from being used for another purpose without their consent;
3) Permit individuals to have access to information pertaining to them in federal records, to have copies made of any or all portions of those records, and to correct any (mis)information in those records;
4) Require federal agencies to collect, maintain, and disseminate any record of information pertaining to identifiable individuals in a manner guaranteeing that such information is accurate and up-to-date for its intended use and requires those agencies to provide adequate safeguards to prevent misuse of those records of information;
5) Allow for exceptions from these protections and requirements only when and where there is an important public policy need for such exceptions; these exceptions must be determined by specific statutory authority;
6) Allows for civil suits to be filed by individuals or groups for damages which result from willful or intentional action(s) in violation of the individuals' or groups' rights defined under this act.

Consumer Privacy Bill of Rights or Internet Bill of Rights

The Consumer Privacy Bill of Rights is not a single piece of legislation, but is instead a term that describes a number of legislative attempts to regulate the processing of electronic personal data in the US. It has also been called a “Privacy Bill of Rights,” or an “Internet Bill of Rights”. These proposed measures would establish consumer privacy as a basic American right- but to date none have been enacted into law.

All of the proposals termed a Privacy Bill of Rights seek to accomplish similar ends. They seek to regulate ***businesses*** that collect personal data from users in order to provide consumers more individual control, privacy, and security when it comes to their data. Themes common to all such measures include:

Security – Businesses are required to responsibly secure and handle personal data

Transparency – Consumers have a right to know what personal data a company has on them, as well as the right to correct those data when inaccurate

Access control – Businesses are limited in how and with whom personal data can be shared with third parties.

Consent – Companies must get opt-in consent from users before collecting, using, or disseminating personal data

Accountability – Government enforcement of the above measures.

Much of the proposed legislation of privacy in general, and Internet privacy in particular, focuses on the regulation and control of data collection, maintenance, and dissemination ***after*** it has been collected. It seems to be assumed that there is a need for public and private agencies and organizations to collect, maintain, and disseminate information about their citizens, clients or users. Existing laws and regulations are concerned with how the information in many databases is put to use once it has been collected. Such laws and regulations provide for punishments following violations.

The issues of the necessity and/or justification for compiling certain databases have not been addressed legislatively. Given the (increasing) volume of information various organizations and institutions have amassed about people and the ease with which such information can be collected, manipulated, and transmitted across the Internet, perhaps an "Internet Bill of Rights" should include a requirement, or at least a strong suggestion, that:

1) Any organization or institution which collects data on people should justify why it is necessary to request information about those people;
2) More particularly, any entity which collects data on people should limit its data collection to those variables which are clearly and directly related to the entity's mission or purpose.

Privacy Issues in Law Enforcement

Government agencies, including law enforcement agencies, have legitimate reasons to infringe on an individual's privacy in the course of collecting information about the individual pursuant to their mission.

Law enforcement is an information-rich activity. There are 3 categories of law enforcement activities in which law enforcement personnel have to deal with information:

1) They have to gather and analyze information to determine if a law has been violated;
2) They have to gather and analyze information to determine the identity of the person or persons responsible for a violation of law;
3) They have to gather and analyze information to support a legal showing in court that the person or persons identified in step 2 are in fact were guilty of the violation.

Concerns about privacy invasions arise from the possibility that law enforcement personnel may investigate more potential suspects than is necessary, or discriminate against certain categories of people in their investigations. In either case, law enforcement agents are tasked with gathering and analyzing information without any specific reason(s) to suspect that these individuals have actually violated some particular law.

The risks that 1) data collection aimed at a particular individual or group of individuals to help in finding out about previously unknown violations of the law, or 2) that the data collected by law enforcement might be used for political purposes or to harass certain individuals or groups, often underlie efforts to restrict not only the kinds of information that law enforcement agencies can gather, but also the way(s) in which it is gathered. Even if the information is never used, the existence of a database containing considerable amounts of data about individuals who have not been accused or convicted of a crime ensures that those individuals may remain on law enforcement's "radar" for long stretches of time. Moreover, such data are a permanent part of their files; citizens may rightly be concerned that this information might eventually be misused or mistakenly released, even if they are not suspects in any crime.

In addition, once an individual is in a law enforcement database, the possibility that he/she may become a suspect or even a "person of interest" should a crime occur can have an effect on an individual's social and economic livelihoods. He/she may not be allowed to fly in a commercial airliner, obtain certain kinds of permits, gain some kinds of employment, obtain financial services, conduct business, perhaps even to contact or have relationships with particular other individuals or groups.

These issues in law enforcement's collection, storage, and dissemination of data on citizens are not new. As an "information-rich activity", law enforcement has had to deal with these problems for decades.

What is new are the modern information technologies that law enforcement agencies can now use to observe situations and identify individuals more quickly, more accurately, and at less expense than ever before. These technologies include surveillance cameras, facial recognition software (still not widely trusted), large-scale databases, and analytical techniques (data mining) that enable the extraction of information from large masses of otherwise irrelevant information.

There is concern that this increasingly sophisticated technology that law enforcement agencies now have available for surveillance, data sharing and analysis, and data storage, combined with a weakening of rules protecting individual information, will allow those law enforcement (and national security) agencies a greatly expanded and largely unseen (or at least unnoticed) ability to monitor all citizens. It is not difficult to imagine the potential for abuse given such an ability. For example, a law enforcement agency might be able to monitor gatherings of groups of citizens objecting to a certain government policy or action, identify who they meet with and perhaps what they talk about.

Adding to such potential abuses, there is often a tendency to believe that the technology is capable of far more than it can actually do. The problem may not lie in what these government agencies can do with the technology, but rather with what citizens believe those agencies can do and/or actually do with it.