MODULE ON THE LEGAL SOURCES OF THE RIGHT TO PRIVACY IN THE CONTEXT OF IDENTITY MANAGEMENT

by
Fenn C. Horton III, Esq.
Pahl & McCay
San Jose, California

April 16, 2009

I. PURPOSE AND OUTLINE OF THIS MODULE

The concept of Aprivacy law@ in the United States is derived from a broad landscape of constitutional, statutory and common law sources. Privacy law has developed over time in response to different threats to privacy that may have prevailed at different times in this nation=s history. Because technology is constantly developing, and the perceived external threats to our national security are continually changing, the scope of the right to privacy is always subject to legitimate debate. A government agency and its individual employees will find it extremely challenging to predict with any certainty whether or not a particular policy or pattern of conduct can successfully be attacked as an invasion of privacy.

The purpose of this module is to provide students, either current or future government officers, a working familiarity with certain legal doctrines that, for the most part, have been applied fairly consistently and the constitutional, statutory and common law sources on which privacy law in this country is based. This module will focus primarily on privacy law as it impacts the use of biometrics by public and private agencies, however, the knowledge gained in this module will be useful in analyzing privacy issues in general. The knowledge the student will gain about privacy law in this module should be applicable to any number of situations in which the right to privacy may arise in public and private enterprises.

In order to gain a more in-depth understanding of the privacy laws implicated by the use of biometrics, students are encouraged to read The National Biometrics Security Project=s Report on United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics (March 2006). This module is intended to supplement that Report.

This module will introduce the student to the full range of constitutional, statutory and common law sources that lay the foundation for the right to privacy so that the student can understand why the distinction between the use of biometrics for identification as opposed to verification is important in analyzing the privacy implications of a government agency=s conduct. This module will also provide the student with a framework for analyzing the privacy implications of specific conduct in the field, and guidelines for creating and implementing a privacy policy for a government agency to follow in collecting, maintaining and using biometrics, as well as other personal information.

The outline of this module will be:

I. Practical Framework for Understanding and Working with the Right to Privacy.
   - A. The identification of government conduct that implicates the right to privacy.
   - B. Analytical framework for tailoring government conduct so as to minimize violations of the right to privacy.

C. The essential elements of an effective privacy policy.

II. Source Materials.
A. United States constitutional sources of privacy law.
B. Federal statutory sources of privacy law.
C. State privacy laws.
D. Common law right to privacy.
E. Survey of initiatives outlining effective privacy policies.

II. ACTIVITIES THAT IMPLICATE THE RIGHT TO PRIVACY

A Surveillance by the government and the secret gathering of personal information.

B. The collection and retention of personal information by the government and private businesses.

C. The use of legally obtained personal information for improper purposes.

D. The use of illegally obtained personal information for legitimate purposes.

E. The absence of any reliable means to verify or contest the accuracy of personal data maintained in a government or private database.

F. The government=s retention of extensive amounts of legally obtained personal information that has no, or a very attenuated, relevance to any legitimate government purpose.

III. ANALYTICAL FRAMEWORK FOR IDENTIFYING THE SCOPE OF THE RIGHT TO PRIVACY

Because of the breadth and complexity of privacy laws as a body of legal knowledge, it is helpful to approach the subject from a specific vantage point. In this module, we will be approaching privacy law from the viewpoint of an employee of a public agency who is intending to use biometric information in carrying out his or her job for the public agency. As discussed in the National Biometrics Security Project=s Report, the privacy implications of the use of biometrics depends on the purpose for which the biometric information is being used and the manner in which it is collected. In their current technological form, biometric recognition systems are used for one of two purposes: (1) to **identify** an individual whose identity is not known by the government agency; or (2) to **verify** that an individual is who he or she says he or she is. The use of biometrics to establish the identity of a person who is being investigated by a government agency implicates the right to privacy because the identification of an individual

through the use of biometrics requires that the government agency maintain, or have access to, a large database of biometric information from people whose identities are known, in addition to the fact that the government agency is searching its database of biometric information without the knowledge or consent either of the person whose identity the agency is attempting to establish or the individuals whose biometric information is stored in the database and scanned.

The use of biometrics to verify the identity of an individual is less controversial from a privacy standpoint because the verification process is usually engaged in with the consent of the individual whose identity is being verified, and there is no need to search large amounts of biometric information from unrelated individuals. The verification procedure consists of matching the biometric information of the person whose identity is being verified with a single biometric template that the agency has previously tagged with that person=s identity.

The All Important Balancing Test

When a court approaches a claim of invasion of privacy made by an individual, regardless of whether the claim is made under the constitution, a statute, or common law, the court will apply a balancing test to determine whether there has indeed been an actionable invasion of privacy for which the government must pay monetary damages or submit to some other judicially enforceable remedy. If a private citizen were to challenge a government agency=s particular use of biometrics, this balancing test would be used by the court in determining whether the government agency should be prohibited from continuing that particular use of biometrics and whether the government should pay the individual claimant monetary damages. The balancing test is a classic example of the Ascales of justice@ being used to arrive at an equitable result in litigation. The ubiquity of this balancing test clearly illustrates that the right to privacy is not absolute and that the protection afforded by the right to privacy, whether constitutional, statutory or common law, is determined by the particular circumstances in which the government impinges on the individual=s autonomy.

The jurisprudence concerning the right to privacy recognizes five spheres of individual autonomy: (1) associational privacy, (2) informational privacy, (3) physical privacy, (4) decisional privacy, and (5) communications privacy. The spheres of autonomy that are most likely to be implicated by the collection, maintenance and use of biometric information are associational privacy, informational privacy and physical privacy. Associational privacy is the right to form friendships and alliances for a variety of reasons, such as, human intimacy, political expression, business pursuits, and recreation. The United States Supreme Court has interpreted the United States Constitution as protecting an individual=s choice to enter into and maintain human relationships against undue intrusion by the government. Informational privacy is the right to control one=s own personal information, such as criminal, financial, and medical records. Physical privacy is the right to control access as to one=s body and personal space, such as, bodily fluids, body cavities and orifices, one=s home, and one=s personal papers and property.

The United States Supreme Court has also interpreted the Constitution as recognizing a right to associate with other people for the purpose of engaging in those activities protected by the First Amendment, i.e., freedom of speech, freedom of the press, freedom of religion, and freedom of association. When biometric information is used by the government for the purpose of identifying the individual members of a particular group that the government is investigating, this right to associational privacy is implicated. One must be mindful of the fact that the human face is a biometric, and the Privacy Act of 1974 prohibits even the collection of such biometric information by the government, unless the collection of such information is directly related to Alaw enforcement activities@, or expressly authorized by statute or the individual whose information is being collected.

Whenever the government engages in activities that intrude upon any of the five spheres of autonomy, the scope of the individual=s right to privacy must be considered and analyzed to determine whether the intrusion is worth the risk of the government agency being subjected to constitutional, statutory or common law claims of violation of the individual=s right to privacy. The resulting litigation can jeopardize government operations because such claims can generate unwelcome publicity, such claims can ruin the careers of the individual government employees involved in the intrusive conduct, and such claims can result in judicially-imposed limitations on the government agency=s future conduct, as well as substantial monetary damages having to be paid which had not been previously been budgeted for.

Once an intrusion on a sphere of autonomy has been described by an individual, the court will apply the balancing test to determine whether the government has engaged in an unreasonable, i.e., actionable, invasion of privacy. In this balancing test, the government=s interest is balanced against the individual=s interest. In some form, the court will engage in the following steps in applying the balancing test:

Step One: Identification of the government=s interest: When the right to privacy has been implicated by the government=s actions, the government=s interest in this context is determined by the nature of the information the government seeks and the purpose for which the government intends to use that information.

Step Two: Identification of the individual=s interest: The individual=s interest is usually more varied depending on the information that is being sought by the government. The individual=s interest is usually identified by the court as an interest in Abeing left alone,@ an interest in autonomy in the expression of political or religious beliefs, autonomy when engaging in human intimacy, or simply preserving the confidentiality of personal information about oneself. When the government collects information about an individual, the government must be concerned not only about collecting an individual=s privately-held information, but also collecting publicly available information that is used to draw conclusions about an individual=s personal characteristics, such as, religious or political beliefs. For a detective to follow an

individual

around with a camera day after day taking photographs of the individual on public streets and in public places, may implicate that individual=s right to privacy if the police detective uses that publicly available information to draw conclusions about the political groups that the individual associates with or the religious congregations that the individual belongs to.

The right to privacy can be implicated by the manner of collection, the manner in which the information is maintained, and the purpose for which the information is collected and/or maintained. To suggest that the government can ignore the privacy implications of the collection of certain information about individuals simply because the information is publicly available and the government does not maintain a Asystem of records@ as defined by the Privacy Act of 1974 evinces a fundamental misunderstanding of the flexible nature of the right to privacy. Whenever a government agency collects information about the citizenry, the government agency would be well advised to assume that the right to privacy is implicated, and, that the balancing test will be applied to the government=s conduct in pursuing the information. Before engaging in such conduct, the government agency should be able to say with confidence that the government=s interest in engaging in such conduct will outweigh the individual=s privacy interests.

Step Three: The government=s interest in obtaining the information is weighed: A number of factors will be considered to determine the weight of the government=s, i.e., public=s, interest in carrying out the challenged action: (1) what is the purpose of the government=s activity? Is it the investigation of a crime, crime prevention, enforcement of the health and safety laws, national security, intelligence gathering, or the compilation of statistical information for census purposes? (2) How useful is the information being sought in achieving the government=s purpose? For example, in a criminal investigation, the government=s interest in obtaining personal data about the suspect is much greater than obtaining information about the suspect=s neighbors or co-workers. How effective will the government=s collection of this information be in achieving the government=s objective? (3) How effective is the method proposed by the government likely to be in actually obtaining the information that the government seeks? Is there a less intrusive alternative available for the government to use in obtaining the information it seeks? For example, in order to identify potential terrorist cells within the United States, the government proposes a program whereby the government monitors everyone=s email, everyone=s telephone calls, everyone=s use of public libraries, everyone=s credit card usage, everyone=s airline ticket purchases, etc. If the government seeks to obtain more information than it really needs to achieve its objective, the government will jeopardize its position in the balancing test because the government will be diluting its own interest in engaging in the proposed activity.

Step Four: The individual=s interest in being left alone is weighed: (1) What is the extent of the individual=s reasonable expectation of privacy in the place the government seeks information from? As an individual moves away from his or her home, the expectation of

privacy lessens, but it is never entirely eliminated. As the individual migrates from places of mostly individual activities, such as, the home, the neighborhood, the private club, the personal automobile, the public phone booth, into more highly regulated and potentially dangerous areas, such as, schools, the workplace, prisons, airports, military bases, etc., the government=s interest in obtaining information about the individual increases. (2) How intrusive is the method proposed by the government for obtaining information? What is the risk that the government=s proposed method for collecting the information is likely to cause permanent injury, pain, trauma or indignity to the individual? (3) Is the technology used by the government to collect the information commonplace and/or readily available to the public? Sense-enhancing technology that is not available to the public will be considered much more intrusive than publicly available technology. (4) How sensitive is the information being sought by the government? What will be the impact on the individual if there is an unauthorized disclosure of the private information? What safeguards has the government established for maintaining the privacy of the information being sought from the individual? Safeguards for protecting the confidentiality of the information can tip the balance in favor of the government by reducing the individual=s interest in keeping the information out of the hands of the government.

Step 5: The court strikes a balance. When one reads appellate court decisions involving the right to privacy, the outcome of this final step is usually foreordained by the weight the court has given to the government's and the individual's respective interests. It is this final step that provides the opportunity for the judge or judges deciding the case to inject their own political, ethical, moral, religious and personal instincts in deciding whether or not the government has overstepped its bounds. It is this final step that makes all litigation over the right to privacy inherently unpredictable.

Privacy jurisprudence clearly recognizes that not all personal information is created equal. Certain personal information, such as medical records, is considered more sensitive than others, such as name, address, and telephone number. Developments in technology and crime patterns have transformed what was previously thought to be non-sensitive information into more sensitive information. For example, the expanded use of the internet for banking and retail purchasing with credit cards has made birth dates, social security numbers, bank account numbers and credit card numbers much more sensitive than they used to be. This fact of life provides further evidence that the scope of the right to privacy is constantly evolving.

With advanced preparation, a government agency that seeks personal information about individuals can take steps designed to tip the balance in the government agency=s favor and lessen the weight of the individual interest in keeping the information from the government. For example, by implementing appropriate safeguards for maintaining the confidentiality of personal information, the government agency can greatly reduce the court=s concern for protecting the individual=s interests in depriving the government of access to particularly sensitive information. In addition, in deciding what specific information is to be collected and how that information is

to be obtained, the government agency should conduct a thorough analysis of all the alternatives available for achieving its objectives so that the agency can demonstrate to a court that the

agency is using the least intrusive alternative, both in terms of the information being sought and the method used for obtaining the information. Finally, the government agency must be able to articulate why it needs the information it seeks, that is, how the collection of such information relates directly to achieving an essential governmental objective.

IV. BASIC ELEMENTS OF A POLICY DESIGNED TO SAFEGUARD PERSONAL INFORMATION MAINTAINED IN A DATABASE SO AS TO MINIMIZE PRIVACY VIOLATIONS - (The Privacy Act of 1974)

The Essential Elements of an Effective Privacy Policy

As discussed above, one important step a government agency can take to increase its chances of success when a court engages in the balancing test is to implement and effectively enforce a privacy policy to safeguard the personal information collected by the agency. In this module, we will be reviewing the system of safeguards outlined in the Privacy Act of 1974 because it is the most comprehensive law that applies to federal government agencies specifically for the purpose of protecting the personal information collected and maintained by those agencies. The Privacy Act is not perfect, but it has survived for over thirty years, with minor amendments, and it has shown itself to be a durable system of safeguards that has largely been accepted by the public. An outline of the major components of the Privacy Act of 1974 follows. The purpose of this information is to provide the student a general but complete outline of the major characteristics of an appropriate privacy policy that should be implemented by every government agency that collects and maintains personal information.

A. No personal information is disclosed without the permission of the person to whom the information pertains, except in certain enumerated situations that clearly relate directly to a legitimate government purpose that is consistent with the purpose for which the information was originally collected.

B. A system for keeping a detailed record of each disclosure.

C. A simple procedure to permit an individual to review their personal information and to request an amendment of the information pertaining to that individual.

D. Establish rules for the collection and maintenance of the information:

- $ Maintain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be

accomplished by statute or Executive Order.

- Collect information to the greatest extent practicable from the subject individual when the information may result in adverse determinations about an individual=s rights, benefits and privileges under government programs.

- Inform each individual whom the agency asks to provide information of the following: (1) the authority under which the information is solicited, (2) the principle purpose for which the information is intended to be used, (3) the routine uses which may be made of the information, and (4) the consequences to the individual of not providing the requested information.

- Publicize the following: name and location of the database; the categories of individuals on whom records are maintained; the routine uses of the records; the policies and practices of the agency regarding storage, retrievability , access controls, retention and disposal of records; the title and business address of the official responsible for the database; the agency procedures whereby an individual can be notified at his request if the agency has records that pertain to him; the procedure for an individual to gain access to the records pertaining to that individual; and the categories of sources of records in the database.

- Establish a system for ensuring the accuracy, relevance, timeliness and completeness of the information as is reasonably necessary to assure fairness in the agency=s making any decision affecting the individual.

- Prior to disseminating any record about an individual to any person, make reasonable efforts to assure that the records are accurate, complete, timely, and relevant for agency purposes.

- Collect no information describing how an individual exercises First Amendment rights without the express authorization of law or of the individual about whom the record is maintained, unless pertinent to and within the scope of an authorized law enforcement activity.

- Make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory government process when such process becomes a matter

of public record.

- $ Establish rules of conduct for persons involved in the design development operation or maintenance of the database, and a program of instruction in such rules.

- $ Establish appropriate administrative technical and physical safeguards to ensure the security and confidentiality of the database and to protect against any anticipated threats or hazards to its security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained in the database.

- $ Publish in advance any new use or intended use of the information.

E. Provide civil remedies enabling an individual to file a lawsuit for monetary damages and injunctive relief against the agency that maintains the database for any violation of the agency=s rules or other laws.

F. Provide criminal penalties against any agency employee who knowingly makes an unauthorized disclosure of personal information contained in the database.

V. INTERPLAY BETWEEN THE PRIVACY ACT OF 1974 AND THE FREEDOM OF INFORMATION ACT (FOIA)

A. The Privacy Act of 1974 applies to any federal government agency that maintains Arecords@ in a Asystem of records.@

1. ARecord@ is defined as Aany item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history 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.@

2. ASystem of records is defined as Aa 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.@

$ OMB Guidelines further define Asystem of records@ as having the following characteristics:

$ an indexing or retrieval capability using identifying particulars built into the system; and

$ the agency must in fact retrieve records about individuals by reference to some personal identifier.

3. AMaintain@ means to maintain, collect, use or disseminate.

4. Disclosure - Agencies are prohibited from disclosing any record which is contained in a system of records to any person or to another agency except pursuant to a written request by or with the prior written consent of the individual to whom the record pertains, unless the disclosure is expressly permitted by the Privacy Act in Subsection 552a(b)(1) through 552a(b)(12).

$ Section 552a(b)(2) expressly permits disclosure of records that are required to be disclosed under FOIA (5 U.S.C. ' 552).

5. Balancing Test under FOIA. The purpose of FOIA is to allow the public to understand the operations and activities of the federal government, and to implement a general philosophy of full disclosure unless the record is specifically exempted from disclosure.

$ In determining whether a particular disclosure of personal information is required under FOIA, a court will use a balancing test similar to Fourth Amendment analysis: the individual=s privacy interest in not having the information disclosed to the public vs. the FOIA interest in shedding light on the government agency=s performance of its duties. DOJ v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

6. Limits on the Collection of Personal Information. Section 552a(e)(7) prohibits an agency from maintaining any record Adescribing how any individual exercises rights guaranteed by the First Amendment [i.e., freedom of speech, the press, religion and association] unless expressly authorized by statute or by the individual about whom the record is

maintained or unless pertinent to and within the scope of an authorized law enforcement activity.@

$ Section 552a(e)(7) prohibits the government=s collection of such information even if the information is **not** kept in a Asystem of records.@ Maydak v. United Sates, 363 F.3d 512 (D.C.Cir. 2004).

$ ALaw enforcement activity@ is construed broadly by the courts and includes any authorized criminal, intelligence or administrative investigation. Nagel v. U.S. Dept. Of Health and Human Welfare, 725 F.2d 1438 (D.C. Cir. 1984).

7. Rules Governing an Agency=s Maintenance of Personal Information.

$ Only Useful Information May Be Maintained. A government agency may only maintain such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President. S U.S.C ' 552a(e)(1).

$ Information Must be Obtained Directly from the Individual. The agency must collect information directly from the subject individual to the greatest extent practicable, when the information may result in adverse determinations about an individual=s rights, benefits and privileges under federal programs. 5 U.S.C ' 552a(e)(2).

$ Notice to the Individual. The agency must inform each individual whom it asks to supply information on the form used to collect the information or on a separate form that the individual can obtain: the authority under which the information is being solicited, the principal purposes for which the information is to be used, the routine uses which may be made of the information, and the consequences of not providing the information. 5 U.S.C ' 552a(e)(3).

$ Safeguards. The agency must establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated

threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained. 5 U.S.C. ' 552a(e)10).

- $ Subsections 552a(e)(1), (2), (3) and (10) are triggered only if the agency actually incorporates the collected information into a Asystem of records.@

8. Biometric information.

- $ Biometric information collected by a government agency that is kept in such a way as to be retrievable by use of an index that tags each piece of biometric information with a particular identifier will be subject to the Privacy Act (and may be subject to public disclosure under FOIA).

- $ If an agency collects biometric information, but does not keep it in a central database, and the information is not retrievable by reference to some particular identifier, the agency=s storage of such biometric information may not be covered by the Privacy Act. But it is difficult to imagine how such information, or the storage of such unretrievable information, could be of any use to the government agency.

- $ The collection of biometric information for the purpose of describing associational behavior (e.g., identification of terrorist cells) is prohibited by the Privacy Act, even if such information is not stored in a Asystem of records@, unless such collection is Apertinent to and within the scope of an authorized law enforcement activity.@

B. The Computer Matching and Privacy Act of 1988 amended the Privacy Act.

1. Government agencies that want to engage in computer matching with the databases of other government agencies must have written agreements with all agencies participating in the matching.

2. The agency must notify applicants or beneficiaries that their records are

subject to matching.

3. The agency must verify the accuracy of the information before taking any action based on the information.

4. The agency must obtain the approval of the Data Integrity Board for all inter-agency matching agreements.

5. The agency must furnish detailed reports to Congress on all computer matching activities.

VI. UNITED STATES CONSTITUTION - Penumbral right flowing from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments

A. Development of the Constitutional Right of Privacy

1. **Associational Privacy** - NAACP v. Alabama, 357 U.S. 449 (1958) (Alabama statute used to compel disclosure of NAACP=s membership lists violated the Due Process Clause of the Fourteenth Amendment).

$ Roberts v. United States Jaycees, 468 U.S. 609 (1984):

$ Freedom of intimate association: AThe choice to enter into and maintain intimate human relationships must be secured against undue intrusion by the State because of the role of such relationships in safeguarding the individual freedom that is central to our constitutional scheme.@

$ Freedom of expressional association: AThe Constitution has recognized a right to associate for the purpose of engaging in those activities protected by the First Amendment@ (i.e., freedom of speech, freedom of the press, freedom of religion and freedom of association).

$ Brandenburg v. Ohio, 395 U.S. 444 (1969):

$ Ohio=s criminal syndicalism statute which made it unlawful to advocate crime or methods of terrorism, or to voluntarily assemble with any group to teach or advocate such conduct.

$ Declared unconstitutional because the statute did not distinguish between assembling with others merely to teach or advocate the need for force and violence and actually preparing a group for violent action; mere advocacy vs. incitement to imminent lawless action.

$ Conviction of KKK leader who had appeared at a cross-burning rally and exhorted the audience, many of whom were armed, to commit violent acts against African-Americans was reversed.

2. **Political Privacy** - Watlein v. U.S. (1957); Sweezy v. New Hampshire (1957)

3. The Aright to anonymity in public expression@ - Talley v. California (1960)

4. **Communications Privacy** - Katz v. U.S., 389 U.S. 347 (1967):

$ Eavesdropping by means of an electronic listening device placed on the outside of a telephone booth, i.e., not included in the Fourth Amendment=s list of protected areas or things (Apersons, houses, papers, and effects@). Nevertheless, citizens have a reasonable and legitimate expectation of privacy in their communications, which is central to the Fourth Amendment. Wiretapping constitutes a Asearch@ for which a warrant is required because wiretapping violates a *subjective expectation of privacy that society recognizes as reasonable*, i.e,. a subjective expectation of privacy that is objectively reasonable.

5. **Decisional Privacy** - Griswold v. Connecticut (1965)- Privacy in personal decisions, e.g., sex and marriage - use of birth control. Substantial right to privacy prohibits criminalization of birth control. First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments create Apenumbral@ right of privacy. Roe v. Wade (1973) - woman=s decision to abort a pregnancy.

6, **Informational Privacy** - Whalen v. Roe (1977)- Fourteenth Amendment protects the privacy of certain information such as sensitive prescription drug data collected by the state in connection with the prescription of

certain drugs that the State considers to be highly dangerous or vulnerable to abuse.

$ New York State law

$ The Constitutionally protected right of privacy involves two types of interest:

$

(1) AThe individual interest in avoiding disclosure of personal matters@ (i.e., informational privacy); and

(2) the Ainterest in independence in making certain kinds of important decisions.@ (i.e., decisional privacy)

$ The U.S. Supreme Court held that the New York law was constitutional because:

$ the State has a legitimate interest in regulating the prescription of drugs that the State reasonably considers dangerous and vulnerable to abuse; and

$ the degree of intrusiveness was minimal because New York=s administrative procedures designed to preserve the confidentiality of the information severely restricted access and made it extremely unlikely that the information would be disclosed to the public

$ In approving this State law that required the collection and maintenance of personal information, the Court did two significant things:

(1) recognized that informational and decisional privacy protections are not limited to criminal investigations;

(2) in balancing the State=s interests against the individual=s right to privacy, the Court considered the State=s reason for the law and examined the measures implemented by the State for safeguarding the information it collected and maintained (i.e., restricted access and criminal sanctions for unauthorized disclosure).

7. Greidinger v. Davis (1993) declared unconstitutional a Virginia law

requiring voters to display social security number in order to vote.

B. Modern Trend in Fourth Amendment Analysis - Warrantless Searches

- Kyllo v. U.S. (2001) (warrant required)
  - Security of the home threatened
  - Sense enhancing technology (thermal imaging device) not in general use by the public was employed to search for marijuana cultivation going on inside private homes
- U.S. v. Kincade (2004) (warrant not required)
  - Mandatory DNA sample taken from individuals convicted of certain federal crimes (e.g., murder, manslaughter, aggravated assault, sexual abuse, child abuse, kidnaping, robbery, burglary, arson) who are incarcerated, paroled, on probation, or on supervised release. DNA Analysis Backlog Elimination Act of 2000.
  - Three exceptions to the warrant/probable cause requirement
    - (1) Exempted areas
      - Searches at the border
      - Prisoner searches
      - Airport
      - Entrance to government buildings
    - (2) Administrative searches
      - Searches of regulated businesses
      - Reduced expectation of privacy/heightened government interest
    - (3) Special Needs
      - Highway checkpoints regarding recent crime
      - Students in extra-curricular activities
      - U.S. Customs officials

- Railroad employees
- Probationer=s residence
- International communications??

(4) Totality of circumstances when there is reasonable suspicion of criminal activity

- Greatly reduced expectation of privacy
- Severity of resulting interference with individual liberty
- Balancing the degree of intrusiveness vs. State interest in obtaining the information; and
- the degree to which the method of searches advanced the State=s interests

- Kansas v. Maass

  - Blood and saliva sample of convicted burglar for identification only of convicted felon

C. Traditional Fourth Amendment Analysis:

- Fourth Amendment: AThe right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.@

  - Individualized suspicion of criminal activity (i.e. probable cause)

  - Searches must be reasonable

    - Whether a particular search or seizure is reasonable depends on the *totality of circumstances*

    - The permissibility of a particular law enforcement practice is judged by balancing the extent of its intrusiveness on the individual=s Fourth Amendment interests against its effectiveness in promoting legitimate State interests

$ Analysis - Rise v. Oregon, 59 F.3d 1556 (9th Cir. 1995) – If no search has occurred, probable cause not required (i.e., no warrant needed), if intrusion is minimal and justified by law enforcement.

- Impact on individual liberty:

- Extent of person=s expectation of privacy
- Offensiveness of the intrusion
- Manner in which the search was conducted (routine vs. unconventional; commonly available technology vs. exotic high-tech device)
- State=s measures for safeguarding the information once it is collected

$ Promotion of legitimate State interests:

$ Degree to which the search accomplishes government purpose - effectiveness in obtaining the information being sought
$ Availability of less intrusive alternatives
$ Reliability of data obtained
$ Legitimacy of the government=s purpose in seeking the information

VII. STATE CONSTITUTIONAL RECOGNITION OF THE RIGHT TO PRIVACY

$ The California Constitution

$ Article I, Section I, provides as follows: AAll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness and **privacy**.@

$ California=s constitutional right to privacy is unusual in that it applies to the private as well as the public sector.

$ Alaska Constitution Article I, ' 22

- Arizona Constitution Article II, ' 8

- Florida Constitution Article I ' 23

    - Government intrusion only
    - Reasonable expectation of privacy

- Hawaii Constitution Article I, ' 6
    - AThe right to privacy shall not be infringed without a compelling state interest.@
    - AThe legislature shall take steps to implement this right.@
- Illinois Constitution Article I, ' 6
    - Fourth Amended restated
    - Genetic Information Privacy Act
        - Section 30 - No disclosure of the identity of any person upon whom a genetic test was done, or the results of a genetic test, in a manner that permits identification of the subject of the genetic test except to:
            - the subject of the test or legal representative
            - any person designated in writing by the subject
            - disclosure limited to persons who have a need to know.

- Louisiana Constitution Article I, ' 6
    - Fourth Amendment restated

- Massachusetts Constitution Chapter 214, ' 1B
    - AA person shall have a right against unreasonable, substantial or serious interference with his privacy.@ Balance each plaintiff=s job duties with the

      nature of the harm sought to be prevented by the employer before determining a remedy.

- Montana Constitution Article II, ' 10
    - Athe right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest

- Rhode Island Section 9-1-28.1

- AIt is the policy of this state that every person in this state shall have a right to privacy which shall be defined to include any of the following rights individually:

  (1) Secure from unreasonable intrusion upon one=s physical solitude or seclusion
    - reasonable expectation of privacy
    - the invasion is offensive or objectionable

  (2) appropriation of name or likeness
  (3) unreasonable publicity
  (4) false light
  - No genetic testing required for employment

- South Carolina Constitution Article I, ' 10
  - Fourth Amendment restated

- Washington Constitution Article I, ' 7
  - ANo person shall be disturbed in his private affairs, or his home invaded without authority of law.@

- Wisconsin ' 895.50
  - AThe right to privacy is recognized in this state.@
  - Genetic testing: no employer may request or require genetic testing as a condition of employment

- Other states that recognize a right to privacy
  - Privacy: Arkansas, Colorado, Connecticut, Delaware, D.C., Florida, Georgia, Idaho, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Mississippi, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio (Ohio Privacy Act), Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Utah, Vermont, Virginia, West Virginia, Wyoming

VIII. FEDERAL LAWS RECOGNIZED AS THE BASIS OF U.S. PRIVACY LAW

A. Children=s Online Privacy Protection Act (COPPA) (15 U.S.C. 6501 et. seq.)

- Designed to give parents control over what information is collected for their children online. Requires operators of commercial web sites and online sources to provide notice and get parents= consent before collecting personal information from children under 13.

B. Drivers Privacy Protection Act of 1994

- 18 U.S.C. 2721 et seq.
- Puts limits on disclosures of personal information in records maintained by DMVs.

C. Fair Credit Reporting Act of 1970 (FCRA)

- 15 U.S.C. 1681-1681n
- FCRA is designed to promote accuracy, fairness and privacy of information in the reports of every Aconsumer reporting agency,@ the credit bureaus that gather and sell information about consumers to creditors, employers, landlords, and other businesses.

D. Family Educational Rights and Privacy Act of 1974 (FERPA)

- 20 U.S.C. 1232g
- Puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funds.

E. Federal Identity Theft Assumption and Deterrence Act of 1998

- 18 U.S.C. 1028
- Makes it a federal crime to use another identify to commit an activity that violates a federal law or that is a felony under state or local law. Violators are investigated by federal agencies, e.g., Secret Service, FBI, Postal Inspection Service, and protected by the DOJ.

F. Federal Privacy Act of 1974

- 5 U.S.C. ' 552a
- Applies to records of federal government and requires certain fair practices regarding maintenance and disclosure of personal information

G. Financial Services Modernization Act, Gramm-Leach-Bliley, Privacy Rule

- 15 U.S.C. '' 6801-6827
- 1990 law permits consolidation of financial service companies and

requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt out of some sharing of personally identifiable financial information with other companies.

H. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- protects privacy of medical information. Applies to health plans, health care clearing houses and health care providers.

I. Telephone Consumer Protection Act of 1991 (TCPA)

- 47 U.S.C. ' 227

- Puts restrictions in telemarketing calls and on the use of auto dialers, pre-recorded messages and fax machines to send unsolicited advertisements.

J. 1986 Electronics Communications Privacy Act

- Title I: Interception of electronic communications
- Title II: Stored Communications Act
  - Restricts access to stored wire and electronic communications and transactional records

K. Video Privacy Protection Act of 1988

IX. SPECIFIC IDENTITY MANAGEMENT LEGISLATION AND REGULATIONS

- Real ID Act (scheduled to take effect May 2008)

- US - VISIT (US Visitor and Immigration Status Indicator Technology)

- Intelligence Reform and Terrorism Prevention Act of 2004
  - Formerly the Computer Assisted Passenger Pre-Screening Program (CAPPS)
  - Secure Flight shifts passengers screening for airlines to the Transportation Safety Administration (TSA)

X. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE

(From the National Science Foundation=s AuthentX Identity Management System, Privacy Impact Assessment (V.1.2) - Nov. 14, 2007.)

- Homeland Security Presidential Directive 12 (HSPD-12) requires improved processes to strengthen Personal Identity Verification (PIV) of all Federal employees and contractors. National Institute of Standards and Technology=s (NIST) Federal Information Processing Standards Publication 201-1 (FIPS 201-1) provides implementation guidance for HSPD-12

- HSPD-12 emphasizes the need to protect privacy of government employees and

contractors.

$ The HSPD requirements for privacy and security controls include:
(1) Naming a Senior Agency Official for Privacy to oversee the privacy protections related to implementation of the Personal Identity Verification (PIV) process
(2) Publishing a Privacy Act statement available to all employees and contractors.
(3) Conducting a Privacy Impact Assessment (PI) of the systems that support the PIV process. This must be submitted to OMB Privacy Officials for review.
(4) Publishing a Privacy Act System of Records Notice (SORN) in the Federal Register, for public comment (current SORN is being amended).

XI. THE COMMON LAW RIGHT TO PRIVACY

$ In addition to statutory protections, the courts have developed common law protections which are grouped under the name Ainvasion of privacy.@

$ The common law causes of action that arise out of a violation of the right to privacy include the following:

$ Appropriation of the name and likeness of another;

$ Unreasonable disclosure of private facts;

$ Unreasonable intrusion upon another=s private seclusion; and
$ Publicity that unreasonably places true facts about a person in a false light.

$ Employer activities that can give rise to common law invasion of privacy claims:

$ The use of photographs or names of employees in the employer=s advertising materials can lead to claims of appropriation of the name and likeness of another;

$ The unreasonable disclosure of an employee=s medical information can lead to claims of unreasonable publicity of private facts;

$ Surveillance of an employee can lead to claims of unreasonable intrusion upon private seclusion; and

$ Disclosure of incomplete details about an employee=s termination can give rise to false light claims.

XII. HISTORY OF PRIVACY INITIATIVES BY THE FEDERAL GOVERNMENT

(From the Testimony of Ari Schwartz of the Center for Democracy and Technology, before The House Committee on Gov=t Reform, Subcommittee on Gov=t Management, Information and Technology, April 12, 2000.)

A. Health Education and Welfare Advisory Committee on Automated Personal Data Systems, 1972

$ In 1972, Elliot L. Richardson, then Secretary of the U.S. Department of Health, Education and Welfare (HEW), appointed an Advisory Committee on Automated Personal Data Systems to explore the impact of computerized record keeping on individuals. In the report published in 1973 the Advisory Committee proposed a Code of Fair Information Practices.

$ The basic principles of the 1973 Code are as follows:

(1) There must be no personal data record-keeping systems whose very existence is secret;
(2) There must be a way for an individual to find out what information is in his or her file and how the information is being used;
(3) There must be a way for an individual to correct information in his or her records;
(4) Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse, and
(5) There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

B. Privacy Protection Study Commission of 1977

$ In 1977, the Privacy Protection Study Commission, charged with studying

the issues raised by the Privacy Act of 1974 and recommending future legislation, issued its report: Personal Privacy in an Information Age.

$ The Commission recommended that Congress pass additional information privacy legislation to protect information held in private sector databases, including a set of Fair Information Practices that employers would voluntarily follow when collecting data about individuals for hiring purposes.

$ The Fair Information Practices are as follows:

(1) Disclosures of Personal Employment Data
- $ An employer should limit external disclosures of information in records kept on individual employees, former employees, and applicants; it should also limit the internal use of such records
- $

(2) Individual Access
- (i) An employer should permit individual employees, former employees, and applicants to see, copy, correct, or amend the records maintained about them, except highly restricted security records, where necessary.
- (ii) An employer should assure that the personnel and payroll records it maintains are available internally only to authorized users and on a need-to-know basis

(3) Informing the Individual
- $ An employer, prior to collecting the type of information generally collected about an applicant, employees, or other individual in connection with an employment decision, should notify him/her as to:
  - (i) the types of information expected to be collected;
  - (ii) the techniques that may be used to collect such information;
  - (iii) the types of sources that are expected to be asked;
  - (iv) the types of parties to whom and circumstances

under which information about the individual may be disclosed without his authorization, and the types of information that may be disclosed;

(v) the procedures established by statute by which the individual may gain access to any resulting record about himself;

(vi) the procedures whereby an individual may correct, amend, or dispute any records about himself.

$ An employer should clearly inform all its applicants upon request, and all employees automatically, of the types of disclosures it may make of information in the records it maintains on them, including disclosures of directory information, and of its procedures for involving the individual in particular disclosures

(4) Authorizing Personal Data Collection

$ No employer should ask, require, or otherwise induce an applicant or employee to sign any statement authorizing any individual or institution to disclose information about him, or about any other individual, unless the statement is:

(i) in plain language;

(ii) dated;

(iii) specific as to the individuals and institutions he is authorizing to disclose information about him;

(iv) specific as to the nature of the information he is authorizing to be disclosed;

(v) specific as to the individuals or institutions to whom he is authorizing information to be disclosed;

(vi) specific as to the purpose(s) for which the information may be used;

(vii) specific as to its expiration date, which should be for a reasonable period of time not to exceed one

year

(5) Medical Records

$ An employer that maintains an employment-related medical record about an individual should assure that no diagnostic or treatment information in any such record is made available for use in any employment decision. However, in

$ certain limited circumstances, special medical information might be so used after informing the employee.

$ Upon request, an individual who is the subject of a medical record maintained by an employer, or another responsible person designated by the individual, should be allowed to have access to that medical record, including an opportunity to see and copy it. The employer may charge a reasonable fee for preparing and copying the record

$ An employer should establish a procedure whereby an individual who is the subject of a medical record maintained by the employer can request correction or amendment of the record

(6) Use of Investigative Firms

$ Each employer and agent of an employer should exercise reasonable care in the selection and use of investigative organizations, so as to assure that the collection, maintenance, use, and disclosure practices of such organizations fully protect the rights of the subject being investigated.

(7) Arrest, Conviction, and Security Records

$ When an arrest record is lawfully sought or used by an employer to make a specific decision about an applicant or employee, the employer should not maintain the records for a period longer than specifically require by law, if any, or unless there is an outstanding indictment.

$ Unless otherwise required by law, an employer should seek or use a conviction record pertaining to an individual applicant or employee only when the record is directly relevant to a specific employment decision affecting the individual

$ Except as specifically required by federal or state statute or regulation, or by municipal ordinance or regulation, an employer should not seek or use a record of arrest pertaining to an individual applicant or employee

$ Where conviction information is collected, it should be maintained separately from other individually identifiable employment records so that it will not be available to persons who have no need of it.

$ An employer should maintain security records apart from other records

(8) General Practices

$ An employer should periodically and systematically examine its employment and personnel record-keeping practices, including a review of:

(i) the number and types of records it maintains on individual employees, former employees, and applicants;

(ii) the items of information contained in each type of employment record it maintains;

(iii) the uses made of the items of information in each type of record;

(iv) the uses made of such records within the employing organization;

(v) the disclosures made of such records to parties outside the employing organization;

(vi) the extent to which individual employees, former employees, and applicants are both aware and systematically informed of the uses and disclosures that are made of information in the records kept about them

C. Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

- In late 1980, the OECD issued Guidelines concerning privacy. the US provided input through a private sector government collaboration headed by the National Telecommunications Infrastructure Administration (NTIA) in the Department of Commerce and the Bureau of International Communications and Information Policy in the State Department

- The OECD guidelines set up important standards for future governmental privacy rules. Although the Guidelines were voluntary, about half of OECD member-nations had already passed or proposed privacy-protecting legislation in 1980. The United States has endorsed the OECD Guidelines.

- The OECD Guidelines are as follows:

  - Collection Limitation Principal
    - there should be limits to the collection of personal date and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

  - Data Quality Principle
    - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date

  - Purpose Specification Principle

- The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- Use Limitation Principle
  - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except:

  (i) with the consent of the data subject; or

  (ii) by the authority of law.

- Security Safeguards Principle
  - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- Openness Principle
  - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- Individual Participation Principle
  - An individual should have the right:

  (i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

  (ii) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him

  (iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

(iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended

$ Accountability Principle

$ A data controller should be accountable for complying with measures which give effect to the principles stated above.

D. Computer System Security and Privacy Advisory Board (CSSPAB)

$ In 1987 Congress established the CSSPAB as a public advisory board as a part of the Computer Security Act. The Computer Security Act specifies that the Board=s mission is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

$ The CSSPAB is composed of twelve members, in addition to the Chairperson, who are recognized experts in the fields of computer and telecommunications systems security and technology. The board examines those issues affecting the security and privacy of sensitive unclassified information in federal computer and telecommunications systems. The CSSPAB=s authority does not extend to private-sector systems or federal systems which process classified information

$ The CSSPAB advises the Secretary of Commerce and the Director of the National Institute of Standards and Technology (NIST) on computer security and privacy issues pertaining to sensitive unclassified information stored or processed by federal computer systems. The Board reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and appropriate committees on Congress.

E. National Information Infrastructure Advisory Council

$ In March 1995, the National Information Infrastructure Advisory Council (NIIAC), was organized into three Mega-Projects: privacy, security, and intellectual property. The Privacy project developed a set of Principles issued in the larger report entitled: AProject Common Ground.@

$ The NIIAC Principles are as follows:

(i) Personal privacy - including information, transactions, and communications - must be protected in the design, management, and use of the National Information Infrastructure (NII). Autonomy and individual choice are fostered by ensuring privacy and by requiring informed consent prior to the use of personally identifiable information on the NII.

(ii) Protection of privacy is crucial to encouraging free speech and free association on the NII; however, such protections are not absolute and must continue to be balanced, where appropriate, by concepts of legal accountability and First Amendment rights.

(iii) To achieve its full potential, the NII must incorporate technical, legal, and self-regulatory means to protect personal privacy. The privacy of communications, information, and transactions must be protected to engender public confidence in the use of the NII. For instance, people should be able to encrypt all lawful communications, information and transactions on the NII. Network-wide and system-specific security systems that ensure confidentiality, integrity, and privacy should be incorporated into the design of the NII. In an interactive electronic environment, transactional information should be afforded a high level of protection.

(iv) Existing constitutional and statutory limitations on access to information, communications, and transactions such as requirements for warrants and subpoenas, should not be diminished or weakened and should keep pace with technological developments. Privacy protections should be consistent across technologies, and should be technology neutral.

(v) At a minimum, existing rights to review personally identifiable information and the means to challenge and correct inaccurate information should be extended into the NII.

(vi) Individuals should be informed, in advance, of other uses and disclosures of personally identifiable information provided by that

individual or generated by transactions, to which that person is a party, on the NII. Personally identifiable information about an individual provided or generated for one purpose should not be used for an unrelated purpose or disclosed to another party without the informed consent of the individual except as provided under existing law.

(vii) Data integrity - including accuracy, relevance, and timeliness of personally identifiable information - must be paramount on the NII. Users of the NII, including providers of services or products on the NII, should establish ways of ensuring data integrity, such as audit trails and means of providing authentication.

(viii) The use of a personal identification system administered by any government should not be developed as a condition for participation in the NII.

(ix) Subject to public policies intended to secure and maintain the integrity and enforceability of rights and protections under U.S. laws - such as those concerning intellectual property, defamation, child pornography, harassment, and mail fraud - spheres for anonymous communication should be permitted on the NII. Those who operate, facilitate, or are otherwise responsible for such spheres must adequately address the sometimes conflicting demands and values of anonymity, on the one hand, and accountability, on the other.

(x) Collectors and users of personally identifiable information on the NII should provide timely and effective notice of their privacy and related security practices.

(xi) Public education about the NII and its potential effect on individual privacy is critical to the success of the NII and should be provided.

(xii) Aggrieved individuals should have available to them effective remedies to ensure that privacy and related security rights and laws are enforced on the NII, and those who use the remedies should not be subject to retaliatory actions.

(xiii) The content and enforcement of privacy policy on the NII should be consistent. A process for overseeing the development,

implementation, and enforcement of privacy policy on the NII should be established. Such process should receive input from all levels of government and the private sector.

F. Information Infrastructure Task Force Principles for Providing and Using Personal Information - 1995

$ New privacy safeguards were needed to respond to the increasing use of computers in data collection. In the U.S., The Information Infrastructure Task Force=s (IITF) Information Policy Committee issued

- Principles for Providing and Using Personal Information in June 1995. The statement of principles included a call for all participants in the National Information Infrastructure to observe several rules:

- Data should not be altered or destroyed improperly;
- Data should only be collected for a specific purpose and should be kept only as long as it is useful for that purpose;
- Individuals should be notified about data collection, including why the information is being collected, how it will be used, how it will be protected, and what will happen if the data is not provided; and
- Individuals should be able to access and correct their information.

///

XIII. HYPOTHETICALS

HYPOTHETICAL CASE NO. 1:

The Federal Bureau of Prisons (BOP) offers a service of taking a photograph of prisoners with their visitors at the request of prisoners for a $1.00 fee paid by each prisoner who wants a photograph. The photo processing service provides one free duplicate. Instead of giving the free duplicate to the prisoner, prison officials keep the duplicate without the prisoner's knowledge. Prison officials keep the duplicate photographs in a box at each prison for six months and then discard them. The duplicate photos are not organized in the box in any particular manner and they are not indexed or assigned individual names or identifying numbers, so there is no system for retrieving the photos once they are placed in the box.

BOP officials review the duplicate photos "for various threats to institution safety or security, for any gang-related activity, for investigative or informative value, or for other conduct." The photos are used to identify possible associates or accomplices of an inmate suspected of, or charged with, criminal acts. One of the primary reasons for keeping the photos is to enable prison officials to track and prevent unlawful activities within the prison.

A group of prisoners found out about the BOP's practice of keeping the duplicate photos and sued the BOP for violating the Privacy Act of 1974. How should the court rule on this claim?

If a newspaper makes a request under the Freedom of Information Act, is the BOP obligated to produce a copy of the photos?

What if a similar practice were being engaged in by a local law enforcement agency and the photographs were being taken of private citizens, out in public, without their knowledge or consent in an area of town in which several gang-style murders had recently taken place? In this area of the city, on a daily basis, the police are taking a photograph of everyone who appears to be between the ages of 15 and 25. The police maintain and review the photos to try to identify patterns of behavior or connections between people. The police have not indexed the photos,

they have no rule on how long they intend to keep the photos, and they have not told the public anything about this practice. What are the legal concerns that this practice gives rise to? What additional information about this practice would you like to know?

Maydak v. U.S., 363 F.3d 512 (D.C. Cir. 2004)

HYPOTHETICAL CASE NO. 2:

The police in San Francisco have begun testing the prototype of a newly developed handheld device that is capable of capturing the fingerprint of any person who touches his or her index finger to the device's screen. The device can then connect via internet to an FBI database and run a search for matching fingerprints.

A serious crime was recently committed and fingerprints were left at the scene of the crime. A witness who was near the crime scene at the time the police believe the crime was committed has provided the police with a description of a man leaving the crime scene. The witness did not see the suspect commit any crime or do anything suspicious other than being present near and leaving the crime scene shortly after the crime may have been committed.

The police have begun searching the entire city and are stopping anyone who fits the description provided by the witness. Are there any constitutional concerns if the police ask each person to stop and place an index finger on the handheld device so the police can search their database for a match? What if a person refuses? Can a person be arrested for refusing to allow the police to scan his or her fingerprint? What should the person be charged with?

Terry v. Ohio, 392 U.S. 1 (1968)

Berkemer v. McCarty, 468 U.S. 420 (1984)

Hiibel v. Sixth Judicial District of Nevada, et al., 542 U.S. 177 (2004)

Kyllo v. U.S., 533 U.S. 27 (2001)

California v. Ciraolo, 476 U.S. 207 (1986)

Katz v. U.S., 389 U.S. 347 (1967)

HYPOTHETICAL CASE NO. 3:

An airline (Friendly Skies) has a practice of compiling and maintaining personal information known in the airline industry as Passenger Name Records (PNRs) on each of its adult and minor passengers. The information in a PNR includes passenger names, addresses and phone numbers and travel itineraries. PNRs are maintained, or temporarily stored, on the airline's computer servers and passengers are permitted to review and modify their stored information. The information in the PNRs is obtained from passengers over the phone or by the internet when the passenger buys a ticket.

In order to encourage passengers to provide this information, Friendly Skies publicizes a privacy policy in which Friendly Skies assures passengers that Friendly Skies will only use computer IP addresses to help diagnose server problems, cookies to save consumer's names, email addresses to alleviate consumers from having to re-enter their information on future occasions, and optional passenger contact information to send the user updates and offers from Friendly Skies. The airline's privacy policy expressly states that any personal and financial information collected by Friendly Skies would not be shared with third parties and would be protected by secure servers. The airline also purported to have security measures in place to safeguard the information.

After September 11, 2001, a private data mining company (Total Info) presented a data pattern analysis proposal to the DOD geared toward improving the security of military installations throughout the U.S. and possibly abroad. Total Info suggested that a rigorous analysis of personal characteristics of people who sought access to military installations might be useful in predicting which individuals pose a risk to the security of those installations. DOD contracted with Total Info to carry out a limited test of its proposed study by adding Total Info as sub-contractor on an existing contract with another private company, and that contract was amended to include PNRs as a possible data source to be used in connection with Total Info's study.

In order to carry out its study, Total Info needed access to a large national-level database of personal information and because none of the federal agencies approached by Total Info would grant access to their government databases, Total Info independently contacted a number of airlines. The airlines declined to cooperate unless the DOT or the TSA were involved and approved the sharing of the information.

Unable to obtain the data on its own, Total Info asked DOT and TSA for help, and both agencies agreed to help. TSA sent Friendly Skies a written request to share its PNRs with Total Info, and Friendly Skies agreed. Friendly Skies sent Total Info 5 million electronically stored PNRs, which then created its own database with the following information: each passenger's name, address, gender, home ownership or rental status, economic status, social security number,

occupation, the number of adults and children in each household, and the number of vehicles owned. Using the data, Total Info created a customer profiling scheme designed to identify high-risk passengers among those traveling on Friendly Skies.

When Total Info's study was made public, Friendly Skies' CEO publicly admitted that it had violated its privacy policy. A class action lawsuit was filed against Friendly Skies and Total Info, seeking compensatory and punitive damages and injunctive relief, based on the following causes of action: (1) violation of the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2701, *et seq*.; (2) violation of state consumer protection statutes; (3) trespass to property; (4) unjust enrichment; (5) declaratory relief; and (6) breach of contract against Friendly Skies.

How should the court rule?

JetBlue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D.N.Y. 2005)

HYPOTHETICAL CASE NO. 4:

The state of New York has enacted a statute that authorizes a police officer to stop an individual and ask the individual to provide a written form of identification. If the stopped individual is unable to provide any identification with a picture, the statute authorizes the police officer to ask the individual to pose while the officer takes a digital photograph of the individual's face. The statute makes it a misdemeanor for any individual to refuse either request, and provides for a fine of up to $500, imprisonment for up to six months, or both. The purpose of the statute is to assist police officers who are investigating a crime in identifying witnesses and suspects by enabling them to compare the digital photograph with a large database of identified photographs maintained by the State of New York State. If the police officer is able to obtain an identification of the photographed individual, the photo is added to the state's database and tagged with the identity of the individual. If the police officer is unable to identify the photographed person, the photo is kept by the state for 30 days, without any identifying information, and then discarded.

The police are investigating a group of "families" who live in a five-unit apartment building in Brooklyn. The police suspect these families of having formed some sort of religious cult, of engaging in polygamy, of having sex with minors, and of plotting terrorist activities targeted at the department of revenue of the State of New York. These suspicions are based on the newspapers, magazines and other mail that neighbors have reported to the police as being delivered regularly to the building.

In order to investigate these people, the police decide to set up a surveillance team in the building across the street to watch who comes out of and goes into the building. When someone comes out of the building, the surveillance team calls one of several patrolmen, who are stationed

at various points several blocks from the building, and alerts the patrolman that an occupant of the building is walking his or her way. The detective on the street then stops the individual and asks for identification. If the person cannot produce a picture id, the detective then asks to take a photograph. Over a two-month period, twenty-eight people are stopped by the police and each one either shows the patrolman a picture id or allows a photograph to be taken. The twenty-ninth person refuses to do either. That person is convicted under the statute described above, fined and jailed. The police then decide to close the investigation without charging anyone with any other crime, such as polygamy, sex with a minor, or engaging in terrorist activities.

After the investigation is closed, The New York Times finds out about it and files a request for information under New York's equivalent to the Freedom of Information Act. In its request, the Times asks for the entire contents of all the files related to the investigation, including any documents related to the police department's rationale for engaging in the investigation and the process for authorizing the investigation, and all the photographs and other information that was collected by the police during this investigation.

What legal issues can you identify in this scenario? What additional information would you like to know? Is the conviction of the individual constitutional? Should the Times be provided some or all of the information it has requested?

Hiibel v. Sixth Judicial District of Nevada, et al., 542 U.S. 177 (2004)

Maydak v. U.S., 363 F.3d 512 (D.C. Cir. 2004)