

Understanding Privacy Laws in Connection With Biometric Identification In the United States and the Rest of World

Presented by:

Herbert R. Fineburg, Esquire: fineburg@efm.net

Erica A. Intzekostas, Esquire: eintzekostas@efm.net

Eizen Fineburg & McCarthy, P.C.

Two Commerce Square, Suite 3410

Philadelphia, PA 19103

(215) 751-9666

www.efm.net

Sources of Privacy Laws

<u>Public Sector</u>	<u>Private Sector</u>
U.S. Constitution State constitutions Federal law State law Common law	----- ----- Federal law State law Common law

Recognized Privacy Rights

<u>Privacy Type</u>	<u>Definition</u>
Informational Privacy	The right to control one's own personal data e.g. criminal, financial, and medical records.
Physical Privacy	The right to control access to one's body and personal space, e.g. search and seizures, Peeping Toms, blood tests, DNA swabs.
Decisional Privacy	The right to make autonomous decisions about one's personal life, e.g. abortions, sexual preference.
Communications Privacy	The right to speak to someone else without being heard by others, e.g. intrusive technological hearing devices.

Constitutional Amendments

Privacy as a Constitutional Right

The First Amendment

“Congress shall make no law ... prohibiting the free exercise [of religion]; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble”

The Third Amendment

“No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.”

The Fourth Amendment

“The 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.”

Constitutional Amendments (continued)

The Fifth Amendment

“No person ... shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”

The Fourteenth Amendment Due Process Clause

“ ... No State shall ... deprive any person of life, liberty, or property, without due process of law”

Factors Used in the Balancing Test

Public Interest	vs.	Individual Privacy Interest
------------------------	------------	------------------------------------

Public Interest: Courts look to whether the public interest is important enough to justify the action.

1. What is the purpose of the action (e.g., criminal investigation, crime prevention, health and safety, national security)?
2. Is the public interest furthered by the action?
3. Does the situation rise to the level of a special need permitting the action without a warrant based on probable cause?

Safeguard Measures: What are the measures used to safeguard the information?

The more sensitive the information, the stronger the safeguards need to be. Strong safeguards can tip the scale in favor of the public interest even if the information is highly sensitive

Reasonable Expectation of Privacy: Courts look to society's views on what is reasonable.

1. Where is the intrusion? There is a diminished expectation of privacy in certain places and situations, such as prisons, schools, and airports.
2. What is the level of intrusion? E.g. what is the extent of the risk, trauma, pain, and indignity of the intrusion?
3. What technology (e.g. sensory-enhancing) is being used? How commonplace is the technology? (e.g. metal detectors)

Sensitivity of Information: How sensitive is the information?

Courts have found certain information to be more sensitive, such as health information, while other information, such as Social Security numbers, less so.

The OECD Guidelines' Eight Privacy Principles

1. *The Collection Limitation Principle.* This principle states that there should be limits to the collection of personal data, and that any such data should be obtained only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual.
2. *The Data Quality Principle.* This principle states that personal data collected should be relevant to the purposes for which it is to be used, and, to the extent necessary for such purposes, should be accurate, complete, and up-to-date.
3. *The Purpose Specification Principle.* This principle states that the purposes for which data is collected should be specified not later than at the time it's collected, and that the subsequent use should be limited to the fulfillment of those purposes or such other purposes that are not incompatible with the stated purposes and as are specified on each occasion of change of purpose.
4. *The Use Limitation Principle.* This principle states that personal data should not be disclosed, made available, or otherwise used for purposes other than those purposes in accordance with the "Purpose Specification Principle" except (a) with the individual's consent or (b) with the authority of law.

The OECD Guidelines' Eight Privacy Principles (continued)

5. *The Security Safeguards Principle.* This principle states that personal data should be protected by reasonable security safeguards against such risks as loss, misuse, unauthorized access or disclosure, and modification.

6. *The Openness Principle.* This principle states that there should be a general policy of openness about developments, practices, and policies with respect to personal data. This principle further states that means should be readily available of establishing the existence and nature of personal data, the purpose of its use, and the identity and location of the data controller. [This principle and the two following it clearly imply that there should be a designated “data controller”.]

7. *The Individual Participation Principle.* This principle states that an individual should have certain rights with respect to his personal data, including (a) the right to receive confirmation from the data controller as to whether the data controller has the individual’s personal information, (b) the right to have data related to him communicated to him within a reasonable time, in a reasonable manner, in an intelligible form, and at a cost (if any) that is not excessive, (c) the right to be given the reason for any denial of any such requests, and (d) the right to seek corrections to his personal data.

8. *The Accountability Principle.* This principle states that the data controller should be accountable for complying with measures that give effect to the above principles. [This principle implies that there should be such accountability and data control measures in place, e.g. in the form of a protocol.]