Compilation of State & Federal Privacy Laws

Published by PRIVACY JOURNAL
an independent monthly on
privacy in a computer age

COMPILATION OF STATE AND FEDERAL POLICY LAWS

1988

(With 1989 Supplement in the back of the book)

By

ROBERT ELLIS SMITH

Published by PRIVACY JOURNAL

An Independent Monthly on Privacy in a Computer Age

Library of Congress Classification Data:
KF1262.A3 176 342'.73'085 76-364384

ISBN 0-930072-05-02

Published by:
PRIVACY JOURNAL
P.O. Box 15300
Washington, D.C. 20003
202/547-2865

ABOUT THIS BOOK

This edition of *Compilation of State and Federal Privacy Laws* includes citations and descriptions of *all* of the laws affecting privacy and data collection that the staff of PRIVACY JOURNAL can find. The texts of representative statutes are included in the appendix. The texts of other statutes may be found in earlier editions of the *Compilation*. If so, we have indicated this at the end of the description of the law. If the full text of the law is in this edition, we have indicated with a black dot.

To order a copy of previous editions of this compilation or a subscription to PRIVACY JOURNAL, use the form on the back page of this book.

We continually publish supplements to describe laws enacted since the publication of our latest edition of the *Compilation*. This is available for $10 from PRIVACY JOURNAL. This *Compilation* is best supplemented by a yearly subscription to PRIVACY JOURNAL, which monthly reports on new laws as they are introduced and as they are enacted.

PRIVACY JOURNAL's survey of state and federal laws affecting the confidentiality of personal information is a continuing project, just as the development of fair information standards is an on-going process in each of the state capitals and in Washington. We began in January 1975 with a pamphlet of state laws, in response to requests we received from several of our readers for a compilation of state privacy laws.

We have collected considerably more statutes in this latest edition. We do not claim to have found every single state statute affecting confidentiality; we hope you will notify us of any we have missed so that we may include them in a later edition.

We do claim to have amassed the nation's only single source of information about confidentiality statutes.

Our hope is to provide a readable book that will give public interest groups, attorneys, citizens interested in privacy, legislators, lobbyists, business persons, and researchers an idea of the diverse sorts of privacy protections that exist in the 50 states.

There are weak laws and strong laws. Protecting privacy can involve many things—from Louisiana's prohibition against being a "peeping Tom" to Connecticut's limit of 34 wiretap orders in a 12-month period.

In this edition, we have added laws on drug testing and AIDS, to reflect recent activity in state legislatures. Laws concerning acquired immune deficiency syndrome (AIDS) may be found in sections on Insurance, Medical Records, or Testing in Employment. There are several new state laws assuring confidentiality of library patrons' records. These will be found in the section on Data Banks in Government.

Laws governing the release of motor vehicle information may be found in that section as well, although most are listed in the section on Mailing Lists. Laws restricting employers' access to, or use of, arrest records are found in Arrest Records or Employment Records, depending on the emphasis. Laws recognizing the confidentiality of communications between patients and medical professionals are found in Medical Records, and those affecting other professionals, like lawyers or clergy, are found in Privileges.

Generally, the first section includes laws that permit the expunction or correction of individual arrest records, especially when no conviction results. The section on Bank Records describes laws that restrict what a financial institution can tell outsiders about a customer's financial affairs. "Credit Reporting and Investigation" includes laws affecting credit bureaus, consumer investigation firms, debt collectors "credit clinics," and users of these services. The next section describes laws, being passed now by just about every state in response to federal regulations, setting disclosure and accuracy policies for criminal justice information systems.

The section on Data Banks in Government includes the ten state laws that permit an individual to see and challenge information about himself or herself in government records, the so-called "Fair Information Practices Acts." Also listed are laws, like Kentucky's and Illinois', that provide partial protections along these lines, but are not properly called "Fair Information Practices Acts."

The section of Employment Records has especially changed since earlier editions, because in the interim several states have enacted laws permitting public and private employees to inspect (and in a few cases, correct) their own personnel files. The Medical Records section has expanded considerably as well, because 18 states now permit a patient to see his or her own medical records, and a half dozen legislatures have enacted confidentiality protections for medical records.

The Miscellaneous section includes laws on the issuing of state identity cards. Under Polygraphing in Employment, we have listed the states (and the District of Columbia) that prohibit the use of lie detectors in employment. We have not included the many court cases and few state statutes that prohibit the use of lie detector evidence in criminal cases.

The next section includes laws recognizing a right to sue for an invasion of privacy based on at least one of the four generally recognized aspects of that tort (listed in "About Privacy" on the next page). The section on Privileges lists the state statutes requiring or authorizing communications between a person and his or her attorney, or doctor, or clergy, or counselor to be kept confidential.

Limits on disclosure of School Records and rights of access by parents or students is generally governed by federal law, except in those states with provisions stronger than the federal law.

Each state has been cited by title (tit.), article (art.), chapter (ch.) and/or section (sec.) so that you may look it up in a statute book, generally a revised (rev.) and annotated (ann.) version, in a law library, or write to the state capitol for a copy. The local public library will usually have your own state's statute books available. We have also printed texts of representative statutes.

Be advised that court decisions enhance or diminish the protections afforded by statutes as written by legislators. Further, regulations drafted by state agencies enhance statutory law. In fact, it is probably in state and federal regulations, which have the force of law, where you will find more reference to protection of confidentiality—and more requirements that various kinds of personal information be recorded. The annotations in most statute books will help in researching court decisions and regulations. It may be that one state provides stronger privacy protection by regulation than a neighboring state does by statute.

Many state laws relating to drug and alcohol, psychiatric, medical and juvenile records have "boiler plate" language requiring confidentiality, and many other states have "freedom of information" or "sunshine" laws that open pub-

lic records to scrutiny but designate certain records (pupil records or welfare records) as exempt from public disclosure. We have provided only representative samples of these statutes, to avoid tedium. And because of the universal nature of the husband-wife and attorney-client privilege, only a few were included in the category on privileges. In addition, since most states have uniformly adopted confidentiality provisions in federal legislation to ensure federal funding for child abuse and parent locator record systems, these provisions were not repeated.

All states have constitutional provisions similar to the First Amendment and Fourth Amendment of the United States Constitution; some have written into their state constitutions specific language protecting the right to privacy.

Robert Ellis Smith

January 1988

Cover by Ben Carlson

ABOUT PRIVACY

Back in 1890, Mrs. Samuel D. Warren of Boston was outraged at the press coverage of her parties. This prompted her husband to team with a fellow law professor, Louis D. Brandeis, to devise "the right of the individual to be let alone." The Warren-Brandeis Harvard Law Review article on the right to privacy became the fountainhead for later law and social policy in the United States, a relatively new and roomy nation where privacy had not previously been a prime concern.

Later, after becoming a U.S. Supreme Court justice, Brandeis called the right to be let alone "the most comprehensive of rights and the right most valued by civilized men," *Olmstead v. U.S.*, 277 U.S. 438 (1928), in dissent to the court's holding that wiretaps were not prohibited by the Fourth Amendment, a decision later overturned.

Courts came to recognize the right of the individual to recover damages when his privacy was invaded because of (1) intrusion upon solitude, (2) public disclosure of private facts, (3) casting one in a false light, or (4) use of one's name or image for another person's profit.

In 1965, the U.S. Supreme Court recognized further that an individual has a *constitutional* right to privacy, based on the Bill of Rights guarantees of free speech and association, freedom from unreasonable searches and seizures, the right to remain silent, the right to have one's house free of soldiers in peace time and unenumerated Ninth Amendment rights "retained by the people." *Griswold v. Connecticut*, 381 U.S. 479 (1965). The Supreme Court decision in 1973 legalizing abortions was based on privacy. The courts will recognize this constitutional right to privacy except when it conflicts with a specific constitutional right of another (a newsworthy family's privacy right does not prevail over a news organ's right to publish). In its decision in 1976, the Supreme Court limited the constitutional right to privacy to "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education" and perhaps personal appearance. *Paul v. Davis*, 424 U.S. 693 (1976).

The Roosevelt Administration's New Deal programs brought with them large-scale government collection of personal data *to determine eligibility* (Social Security, veterans benefits, etc.). Government began to collect even more personal information in the 1960s to *to evaluate* effectiveness of programs.

Private business increased its data collection in the mid-20th Century as well, in a population relying on credit purchases (an estimated 55 percent of retail sales are made on credit), insurance (78 percent of all Americans now carry health insurance) and mobility (35 percent of all Americans no longer live in the community where they were born and thus are not known to merchants).

With the need for more personal information came an easier way to gather, store and organize it: computers. What once rested in a manilla folder now could be transferred at great distances, analyzed more cheaply, stored in a fraction of the space and retrieved instantaneously. A computer record can also appear more accurate than it really is and can be used for decisions about you without any human intervention.

The number of computer data banks became staggering by the 1970s: Social Security Administration, Federal Bureau of Investigation, Internal Revenue Service, state motor vehicles departments, National Driver Registry, drug abuse data acquisition projects, Retail Credit Co., Medical Information Bureau, Tenant Reference Guide, TRW Credit Data, Educational Testing Service, state criminal justice information systems, municipal data systems, Veterans Administration, military, state welfare departments, corporate personnel offices, programs for the handicapped, regional mental health programs, Professional Standards Review Organizations for health care evaluation, National Parent Locator, child abuse projects, national church organizations, credit card companies, telephone companies, Passport Office, Immigration and Naturalization Service, state university systems, Medicaid, and more.

Citizens demanded protection. They called it privacy, but what they really wanted was *minimal data collection, accuracy, the right to see and correct their own records, notice before their data was shared with others, and the right to know which data banks exist.*

Common law privacy protections were not enough. The Fair Credit Reporting Act of 1970 covering credit investigating companies required, for the first time, that data gatherers grant access, provide notice, limit disclosure and publicly announce their data collection.

The Swedish Data Act of 1973, articulating virtually the same principles and adding a data inspection board to oversee record-keeping, became a model. The Department of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems in July 1973 and the International Business Machines Corp. in 1973–74 gave their blessings to the same privacy principles.

Variations on the Swedish law, affecting state government records, were passed in Minnesota in April 1974 and in Utah, Arkansas and Massachusetts in 1975, in Ohio, Virginia and Connecticut in 1976, and have been introduced in at least a dozen other states. West Germany in 1976; France, Norway, and Denmark in 1978; and Austria and Luxembourg in 1979 passed privacy laws affecting private and public record-keeping.

In 1978 Canada enacted a Human Rights provision with privacy protections for federal records. In the U.S., the Family Educational Rights and Privacy Act of 1974 required that federally supported school systems and colleges adopt the same principles with regard to school records. The same standards now apply to federal agencies' records on individuals, because of the Privacy Act of 1974.

ABOUT PRIVACY JOURNAL

PRIVACY JOURNAL, an independent newsletter, has been published monthly in Washington since November 1974. *The Washington Post* called it "the most talked about Washington newsletter since *I. F. Stone's Weekly*." A sample copy is available upon request, and back issues are available for sale.

PRIVACY JOURNAL also maintains an extensive research collection of materials about privacy, in each of the areas cited in this book. For a fee, readers may take advantage of this Washington-based research service and receive materials as they need them.

During this year and next, many states will be considering legislation in each of the areas mentioned in this compilation. PRIVACY JOURNAL will be monitoring those developments, and so we urge you now to reserve a copy of a future edition of our compilation of state and federal laws. Simply send us a note now (see the last page of this book) and we'll notify you when a new edition is published.

PRIVACY JOURNAL Publisher Robert Ellis Smith is the author or *Privacy: How to Protect What's Left of It*, a 346-page hardcover book describing the personal information that is gathered by government agencies and commercial organizations like insurance companies, credit bureaus, banks, and mailing houses. It also includes specific advice on how consumers may protect their privacy in an electronic age. The book, published by Anchor Press/Doubleday, is sold by mail by PRIVACY JOURNAL. *The New York Times* called *Privacy* "an absolutely essential book for our time."

You may order the following materials from PRIVACY JOURNAL:

One year subscription

1978-79 Compilation of State and Federal Privacy Laws ($14.50).

1981 Compilation of State and Federal Privacy Laws ($19).

1984-85 Compilation of State and Federal Privacy Laws ($22).

Supplement to the current edition ($12).

Privacy: How to Protect What's Left of It by Robert Ellis Smith ($11).

Workrights, a complete description of laws assuring individual rights of employees ($9.95).

The Big Brother Book of Lists, trivia and anecdotal items on privacy and surveillance ($6.95).

Celebrities and Privacy, a report on legal protection of famous persons' names and images ($14.95).

PRIVACY JOURNAL's *Compilation of State and Federal Privacy Laws* was written and edited by Robert Ellis Smith, publisher of PRIVACY JOURNAL.

CONTENTS

CONTENTS

Jurisdiction	Arrest records	Bank records	Cable	Computer crime	Credit reporting and investigation	Criminal justice information systems	Data banks in Government	Employment records	Insurance	Mailing lists	Medical records	Miscellaneous	Polygraphing in employment	Privacy statutes/ state constitutions	Privileges	School records	Social security numbers	Tax records	Telephone solicitation	Testing in Employment	Wiretaps
Alabama	✓	✓		✓		✓	✓				✓		✓		✓					✓	✓
Alaska		✓		✓		✓	✓				✓		✓		✓				✓	✓	✓
Arizona	✓			✓	✓	✓	✓			✓	✓		✓	✓		✓		✓	✓	✓	✓
Arkansas						✓	(a)				✓		✓						✓	✓	✓
California	✓	✓	✓	✓	✓	✓	(a)	✓	✓		✓	✓	✓	✓		✓			✓	✓	✓
Colorado	✓			✓		✓	✓				✓				✓	✓		✓	✓	✓	✓
Connecticut	✓	✓	✓	✓	✓	✓	(a)	✓	✓		✓	✓	✓		✓	✓		✓	✓	✓	✓
Delaware	✓			✓		✓		✓			✓		✓	✓	✓	✓		✓			✓
District of Columbia	✓		✓				✓	✓	✓		✓		✓								✓
Florida	✓	✓		✓	✓	✓	✓	✓		✓	✓			✓		✓	✓		✓		✓
Georgia	✓			✓	✓	✓			✓		✓		✓	✓	✓		✓	✓	✓		✓
Hawaii	✓			✓		✓		✓		✓	✓	✓	✓	✓				✓			✓
Idaho		(c)		✓		✓					✓		✓		✓	✓		✓			✓
Illinois	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓			✓		✓
Indiana	✓			✓		✓	(a)			✓	✓	✓			✓		✓				
Iowa		✓		✓		✓	✓	✓			✓		✓			✓			✓	✓	✓
Kansas				✓	✓	✓	✓		✓	✓	✓							✓			✓
Kentucky	✓			✓	✓		✓				✓			✓	✓	✓		✓			✓
Louisiana	✓	✓		✓		✓	✓		✓		✓		✓	✓	✓	✓		✓			✓
Maine		✓			✓	✓	✓	✓	✓		✓		✓	✓		✓	✓	✓			✓
Maryland	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓		✓	✓		✓
Massachusetts	✓	✓		✓	✓	✓	(a)	✓			✓	✓	✓	✓	✓	✓		✓	✓		✓
Michigan				✓		✓	✓	✓			✓		✓		✓	✓			✓		✓
Minnesota	✓			✓		✓	(a)			✓	✓		✓		✓	✓		✓	✓	✓	✓
Mississippi				✓			✓				✓		✓		✓	✓					
Missouri	✓			✓			✓				✓				✓						
Montana				✓	✓	✓	✓			✓	✓		✓	✓	✓	✓				✓	✓
Nebraska				✓		✓	✓					✓	✓	✓	✓	✓		✓	✓		✓
Nevada	✓			✓			✓	✓		✓	✓		✓		✓	✓					✓
New Hampshire		✓		✓	✓	✓	✓	✓			✓										✓
New Jersey	✓	(c)		✓		✓	✓		✓		✓		✓		✓	✓					✓
New Mexico	✓			✓	✓	✓							✓		✓						✓
New York	✓			✓	✓		(a)	✓		✓	✓	✓	✓	✓	✓	✓		✓			✓
North Carolina		(c)		✓		✓	✓	✓			✓				✓	✓		✓	✓		✓
North Dakota				✓			✓				✓	✓				✓		✓			✓
Ohio	✓			✓		✓	(a)	✓			✓				✓	✓		✓			✓
Oklahoma		✓		✓	✓	✓	✓				✓		✓	✓	✓	✓	✓	✓			✓
Oregon	✓	✓		✓		✓	✓	✓			✓	✓	✓		✓	✓		✓	✓	✓	✓
Pennsylvania	✓			✓			✓	✓			✓		✓	✓							✓
Rhode Island	✓			✓			✓	✓			✓		✓	✓	✓	✓		✓		✓	✓
South Carolina	✓			✓		✓	✓		✓				✓	✓				✓			
South Dakota				✓			✓	✓			✓				✓	✓		✓			✓
Tennessee	✓			✓		✓		✓			✓		✓	✓	✓	✓		✓			✓
Texas				✓	✓						✓		✓		✓	✓			✓		✓
Utah	✓	✓		✓	✓	✓	(a)	✓			✓		✓	✓	✓			✓		✓	✓
Vermont								✓		✓	✓	✓	✓					✓		✓	
Virginia	✓			✓	✓	✓	(a)		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Washington	✓			✓		✓	✓	✓		✓	✓		✓	✓	✓	✓		✓			✓
West Virginia	✓						✓				✓		✓					✓			✓
Wisconsin	✓		✓	✓			✓	✓			✓	✓	✓	✓	✓	✓		✓	✓		✓
Wyoming				✓			✓				✓				✓	✓			✓		
Federal		✓	✓	✓	✓	✓	(a)	✓	✓	✓	✓	✓		✓		✓	✓	✓		✓	✓

[a]Fair Information Practices Acts.

[c]Significant court decision affecting privacy.

ARREST RECORDS

Alabama—An individual may have access to his or her criminal record. Ala. Code 41-9-643.

Arizona—Any person wrongfully arrested, indicted or otherwise charged may petition superior court for an entry of notation upon any and all records that that person has been cleared. Ariz. Rev. Stat. sec. 13-1761.

California—Whenever a person is acquitted of a charge and it appears to a judge that the person was factually innocent of the charge, the judge may order the records in the case sealed and later destroyed. The person may then state that he was not arrested. Cal. Penal Code sec. 851.8. Records of arrest, records prior to 1976 may be destroyed upon petition to a court. Cal. Health & Safety Code sec. 11361.5.

Law enforcement agencies may not disclose criminal history information with the intent of affecting a person's employment prospects. Cal. Labor Code sec. 432.7(f)(l). Public and private employers may not inquire into arrests of applicants, nor may public agencies inquire into arrests on applications for a license, certificate or registration. Cal. Labor Code sec. 432.7 and Cal. Bus. & Prof. Code sec. 461. Nor may auto insurers inquire. Cal. Ins. Code sec. 11580.08. Mere detentions, not regarded as arrests, must be accompanied by a record of release and the individual is entitled to a certificate labeling the incident a detention. Cal. Penal Code 851.6(b).

For a complete description of the state's laws on arrest records, see *Loder v. Municipal Court*, 17 Cal. 3d at 869 (1976).

Colorado—Any person may petition the appropriate court to seal his or her record, except for basic identifying information, if the person is not guilty of an additional crime within a certain number of years. Employers and educational institutions may not inquire about sealed records. Colo. Rev. Stat. sec. 24-72-308.

Connecticut—State law mandates erasure of all court and police records of arrests, including photos and fingerprints, of persons acquitted, pardoned, dismissed or not prosecuted. Conn. Gen. Stat. Ann. sec. 54-142a. See also Employment Records.

Delaware—For $5, a person may receive a copy of his or her Delaware criminal history record: Del. Code tit. 11, sec. 8511(4). There is a procedure for expunging records. Tit. 11, sec. 4371.

A court may order destruction of a record if there is no conviction and there is no prior record. Tit. 11, sec. 3904.

District of Columbia—Police records of complaints are open to public inspection and the police commissioner may order obsolete records destroyed. D.C. Code sec. 4-131. There is a right to expunge by court order.

Florida—Fla. Stat. Ann. sec. 901.33 provides a right for the expunction of arrest records of acquitted or released persons. [See 78–79 book.] Illegal to discriminate in public employment on the basis of a prior conviction unless it is directly related to the position sought. Sec. 112.011.

Georgia—Arrest information may be disclosed to certain employers and others, but an individual rejected on that basis has a right to be told of the information disclosed. Ga. Code Ann. sec. 35-3-34.

Hawaii—"The attorney general, upon application from a person arrested for, but not convicted of, a crime, shall issue an expungement order annulling, canceling, and rescinding the record of arrest." The record must then be placed in a confidential file in the attorney general's office or erased from magnetic tape or computer memory, to be seen again only under court order. The individual is provided a certificate of annulment and may answer inquiries about an arrest record in the negative. Haw. Rev. Stat. 831-3.2. An individual may not be denied a state job nor license to do business solely because of a criminal conviction. Government employers and license issuers may not use arrest records for which no jail term may be imposed. Other convictions may be considered if job-related. Haw. Rev. Stat. 831-3.1.

Illinois—A person charged but not convicted may petition a court for expunction of the arrest record. Criminal records are generally not public. Ill. Ann. Stat. ch. 38, sec. 206-5 and 206-7. Ch. 68 sec. 2-103 makes it a civil rights violation to inquire whether a job applicant has ever been arrested. A distinction is drawn between arrests and convictions.

Indiana—Upon written request of an individual with no prior arrests and no other criminal charges pending, a law enforcement agency must destroy or return fingerprints and photographs connected with an arrest in which no charges were pressed. The agency must also request any other agencies to which it has sent the arrest materials to do the same. And no record of the arrest may be kept in an alphabetical file. IC 35-4.8.

Kentucky—Individuals have access to their own arrest records. Ky. Rev. Stat. Ann. sec. 61.884.

Louisiana—La. Rev. Stat. Ann. sec. 44:9 provides for the destruction of misdemeanor records for persons later acquitted or released.

Maryland—An individual may answer arrest record inquiries in the negative if acquitted, not prosecuted or dismissed and if he had petitioned a court to seal his record—either three years after the arrest, or if earlier, when he waives his right to civil claims arising from the incident. An employer may not fire a person if he discovers such arrest information. Md. Ann. Code art. 27, sec. 735-741 and art. 27, sec. 292(a).

Massachusetts—Employers must notify applicants that they may respond "no record" if they have been arrested but never convicted; if they have not been convicted within five previous years and have only misdemeanors more than five years old on their records; or if they have only one conviction for simple assault, traffic offenses or drunkenness (misdemeanors). The law applies also to university admissions applicants. Offenders may have criminal records sealed 15 years after release for a felony, 10 years after release for a misdemeanor. Mass. Gen. Laws Ann. ch. 276, sec. 100 A–C. First convictions for marijuana and other drug offenses may be sealed under certain circumstances. Ch. 94C, sec. 34.

Michigan—See Employment Records.

Minnesota—Records of arrests without conviction, convictions that have been expunged, and misdemeanors without jail sentences shall not be used by the state in connection with any application for public employment or license. Minn. Stat. Ann. sec. 364.04.

Missouri—Arrest records are to be sealed if no charge is filed within 30 days. They are then unavailable to the public. Mo. Ann. Stat. sec. 610.100.

Nevada—Fifteen years after release from custody for felony, 10 years after release for gross misdemeanor, 5 years after release for misdemeanor an individual may petition court to seal all records. Nev. Rev. Stat. sec. 179.245. Thirty days after acquittal or dismissal of charges a person may petition for sealing. Sec. 179.255.

New Jersey—Person convicted (except for serious offenses) may petition a court, ten years later, to expunge the record, if there is no law enforcement objection. N.J. Rev. Stat. sec. 2A:164-28.

New Mexico—Criminal records of arrests not followed by valid conviction and misdemeanor convictions not involving moral turpitude shall not be used, distributed or disseminated in connection with an application for any public employment, license or authority. Convictions may be considered but are not a bar to employment. N.M. Stat. Ann. sec. 28-2-3.

New York—Upon termination of a criminal proceeding against a person in favor of that person, all records are sealed unless the district attorney shows the court cause not to, or the person applies for a gun license. It is an unlawful discriminatory practice to inquire about the proceeding. N.Y. Crim. Proc. Law sec. 160.50 (McKinney). Marijuana misdemeanors shall be sealed by a court, even if there is a dismissal. Sec. 170.56.

It is unlawful for an employer, insurance company, or credit bureau to inquire into an arrest that resulted in a favorable outcome for the individual. N.Y. Exec. Law 296.16.

Ohio—First offenders may petition a court for expunction of convictions after release. Ohio Rev. Code Ann. sec. 2953.32. Applicants are not to be asked about expunged criminal records. An applicant may respond in the negative if an employer or licensing body asks about expunged or sealed criminal records. Sec. 2953.43. Similar requirements apply to juvenile records. Sec. 2151.358 (I) and (J).

Oregon—First offenders may petition the court after release for the conviction to be set aside so that it is "deemed not to have ocurred." Or. Rev. Stat. sec. 137.225. An employer must notify a person before getting access to criminal records. 181.555(2). Arrest records are not subject to disclosure if there is a good reason to delay. 192.500(1)(c).

Pennsylvania—Arrest information may not be used for licensing. Only criminal information relevant to the employment may be used in hiring decisions, and the applicant shall be notified when this is done. Pa. Stat. Ann. tit. 18, sec. 9124.

Rhode Island—State law requires destruction, within 45 days of acquittal, of any fingerprints, photographs, and other records of the accused taken by law enforcement. R.I. Gen. Laws sec. 12-1-12. An employment application form may inquire into convictions, but not arrests. 28-5-7(7).

South Carolina—Arrest records and accompanying fingerprints and mug shots shall be destroyed if no conviction. S.C. Code sec. 17-4.

Tennessee—Upon petition to a court, arrest records may be destroyed if there is no finding of guilt, but "non-public" law enforcement records remain. Tenn. Code Ann. sec. 40-32-101. See also 40-15-106.

Utah—Arrest records may be sealed one year after a charge has been dropped. An individual not convicted within five prior years may petition a court to expunge a prior conviction. Utah Code Ann. sec. 77-35-17.5.

Virginia—Similar to Maryland's law. Code of Va. 19.2-392.4(A).

Washington—An individual may ask a court for destruction of records after release or acquittal. Wash. Rev. Code Ann. sec. 43.43.730.

West Virginia—An individual is entitled to have returned to him arrest records, fingerprints and photographs in state files, if he is acquitted. W.Va. Code sec. 15-2-24(h).

Wisconsin—Employment law prohibits inquiring into arrest records, except for bonding. Wis. Stat. Ann. sec. 111.335.

BANK RECORDS

Alabama—A bank shall disclose financial records of its customers pursuant to a lawful subpoena, summons, warrant, or court order issued by or at the request of a governmental agency. No bank shall be held civilly liable or criminally responsible for disclosure of financial records pursuant to such legal process when it appears on its face to be valid. A note to the law says that customer records should be disclosed only upon legal process. Ala. Code 5-5A-43.

Alaska—All books and records of savings and loan associations pertaining to accounts and loans of members shall be kept confidential. Alaska Stat. sec. 06.30.120. Bank records are confidential and shall not be made public except by court order, as required by state or federal law, when authorized, or to holder of negotiable instrument. As amended in 1976, when disclosure is required the depositor must be notified unless disclosure is made under a search warrant. Sec. 06.05.175.

California—Bank customer is entitled to a 10-day notice before a state investigator can obtain records about the customer's financial affairs from the bank. Notice not required if judge determines that law or state regulation has been or is about to be violated. Cal. Gov't Code sec. 7460. Amended in 1978 and 1979.

Connecticut—A customer's records may not be disclosed by a financial institution without legal process or other specifically listed circumstances. Conn. Gen. Stat. Ann. sec. 36-9j.

Florida—*Milohnich v. First Nat'l Bank of Miami Springs*, 224 So. 2d 284 (Fla. 1969), states a rule of bank secrecy except to comply with government orders or to exchange credit data.

The state may require banks operating electronic funds transfer systems to inform customers of their protection policies including "protection against wrongful or accidental disclosures of confidential information." In its annual report, a bank must "disclose procedures for the protection of a customer's privacy and confidentiality of account information and discuss who has access to a customer's account information and under what circumstances." Social Security numbers may not be used as a personal identifying number in electronic systems. Fla. Stat. Ann. sec. 659.062.

Idaho—*Peterson v. Idaho First Nat'l Bank*, 83 Idaho 578, 367 P.2d 284 (1961), says the bank, as the customer's agent, owes a duty of confidentiality.

Illinois—Bank disclosure of customer information is prohibited without customer authorization, a subpoena or regulatory agency request, or credit exchange. $1000 fine. Ill. Rev. Stat. Ann. ch. 16½, sec. 148.1.

Iowa—Satellite terminals or data processing centers are not to permit any person to obtain information concerning the account of any person with a financial institution, unless such information is essential to complete or prevent the competion of a transaction then being engaged in through the use of that facility. Iowa Code Ann. sec. 527.10.

Louisiana—Financial institution or credit card company may release personal credit or financial information only under subpoena with advance notice to the customer, except for exchanges among credit grantors and other businesses and for non-tax law enforcement investigations. La. Rev. Stat. Ann. sec. 9:3571.

Maine—Bank records are confidential, except for matching of government records, for supervisory audit, with consent of the individual, or by legal process. 9-B Me. Rev. Stat. 161.

Maryland—Fiduciary institution may not disclose any financial records unless customer has authorized disclosure or unless records are subpoenaed; subpoena must be directed to institution and customer 21 days prior to disclosure, Md. Ann. Code art. 11, sec. 225.

Massachusetts—No person may (1) condition the extension of credit on participation in an electronic fund transfer system, (2) require a consumer to accept an electronic fund transfer service or establish an account as a condition of employment or receipt of government benefits, or (3) condition the sale of goods or services of a customer's paying by electronic means. A provider of EFT services may not disclose customer information except to the customer or with his authorization, to a party to the transaction, to government regulators, to auditors, to a consumer reporting agency, to the representative of a collection agency, or pursuant to legal process. There must be "reasonable procedures" to prevent unauthorized disclosure. Mass. Gen. Laws Ann. ch. 167-B-7. Banks are required to disclose, when requested by the state, the amount of deposits held by a recipient of, or an applicant for, public assistance. Fine of $50. Mass. Gen. Laws Ann. ch. 18, sec. 15.

New Hampshire—No state or local investigator may get "financial or credit" information about an individual from a financial institution or credit reporting agency unless "described with particularity and consistent with the scope and requirements of the investigation." N.H. Rev. Stat. Ann. sec. 359-C.

New Jersey—*Brex v. Smith*, 146 A. 34 (Ch. N.J. 1929), says "unauthorized prying" into a bank account is a tortious invasion of privacy.

North Carolina—*Sparks v. Union Trust Co.*, 256 N.C. 478, 124 S.E. 2d 365 (1962), implies that bank depositors have a right of confidentiality.

Oklahoma—"A financial institution is prohibited from giving, releasing or disclosing any financial record to any [state] government authority unless it has written consent from the customer for the specific record requested; or it has been served with a subpoena" and a copy of the subpoena is served on the customer before it is served on the financial institution. The customer has 14 days to challenge the demand for his or her financial records. Okla. Stat. Ann. tit. 6, sec. 2201–2206. [See 1981 book.]

Oregon—State law prohibits a financial institution from disclosing customer information to a state or local agency, unless there is a suspected violation of law, unless the customer consents, or unless the government follows procedures similar to those in the federal Right to Financial Privacy Act. Or. Rev. Stat. sec. 192.550.

Utah—Any bank may report to any other bank or credit reporting agency in the state that an "unsatisfactory demand deposit account has been closed out." No liability for any error or omission in such reports. Utah Code Ann. sec. 7-14-1.

Federal law—The Tax Reform Act of 1976 requires that the Internal Revenue Service provide a customer 14 days' notice when it issues an administrative summons to see his records at a bank or other financial institution. After receiving this notice, the customer then has a right to intervene in any proceeding with respect to enforcing the summons and may suspend compliance with the summons if he notifies IRS and the bank within the 14-day period. In that case, a federal district judge will decide on whether to enforce the summons. The court may allow IRS to waive the notice requirement in exceptional circumstances. The new law also requires IRS to notify a court when it seeks the financial records of a class of persons under a "John Doe" summons without specific names. Credit unions, consumer reporting agencies, credit card companies, brokers, attorneys and accountants are subject to these same provisions when they are holders of a third party's business records. 26 U.S.C. 7609. [See 78–79 book.]

Under the Right to Financial Privacy Act of 1978, nearly all federal investigators must present proper legal process or "formal written requests" to inspect the financial records of an individual kept by a financial institution, including a credit card company. The federal agent must give simultaneous notice to the individual, who then has an opportunity to challenge the access. An amendment in 1979 relieved financial institutions of the responsibility to notify customers of these protections. 12 U.S.C. 3401. [See 1981 book.]

The Electronic Fund Transfer Act, effective May 1980, requires institutions operating electronic banking services to inform customers of the circumstances under which automated-banking account information will be disclosed to third parties in the ordinary course of business. 15 U.S.C. 1693c(a)(9). See also 12 C.F.R. 205.10.

CABLE TELEVISION

California—State law prohibits a cable television corporation from using any electronic device to record, transmit, or observe events inside a subscriber's premises and from disclosing any information regarding a subscriber, without consent. Companies may sell simple lists of subscribers and addresses if they permit a subscriber to be deleted from such lists. Customers have a right to inspect and correct information about themselves. Cal. Penal Code 637.5. [See 1984-85 book.]

Connecticut—It is illegal to install a device to observe or listen inside a residence without the knowledge or permission of the cable television subscriber; to release subscriber lists unless subscribers have a chance to delete their names; to disclose subscribers' viewing habits without consent; and to install security scanning devices without express written consent. Conn. Gen. Stat. Ann. 53-421.

District of Columbia—A provider of cable television services shall not install any equipment that permits transmission of an aural, visual, or digital signal from the subscriber's premises without written permission of the subscriber. "The franchisee shall exercise the highest possible standard of care in protecting the privacy of data in its possession with respect to an individual subscriber's financial transactions, viewing selections, and utilization of other computer-based interactive services. This individual subscriber data shall not be subject to subpoena or other compulsory process." D.C. Code sec. 43-1845. [See 1984-85 book.]

Illinois—It is unlawful for a cable company to use equipment that would permit observation or listening inside the household; to provide any private or public organization with a list containing the name of a subscriber, unless prior notice is given subscribers; to "disclose the television viewing habits of any individual subscriber" without consent; or to install any scanning device within a home without written consent. Ill. Ann. Stat. ch. 38, sec. 87-2 [See 1984-85 book.]

Wisconsin—Every cable TV connection must have a device allowing the subscriber to shut off completely any reception or transmission. "No person may intrude on the privacy of another" by, without consent, monitoring use of a subscriber's equipment, disclosing names or addresses that describes behavior or viewing habits, conducting covert research over the system. List may be disclosed if the subscriber has a "negative check-off" option to be deleted. Wisc. Stat. Ann. 134.43. The wiretap law covers cable communications. 968.27(1). [See 1984-85 book.]

Federal law—Cable operators must abide by a code of fair information practices and provide a subscriber with the opportunity to limit disclosure of name and address for mail solicitation and similar purposes. In no case may a cable television company release viewing choices, retail transactions, or other personally identifiable information, without written or electronic consent. A subscriber may check information on file about him or herself for accuracy. Aggrieved individuals have a right to sue for damages. A governmental entity may obtain personally identifiable information only pursuant to a court order based on clear and convincing evidence that the subject of the information sought will be material evidence ***and*** if the subscriber has had an opportunity to be heard to contest the government's claim. 47 U.S.C. 551, enacted in 1984 (P.L. 98-549).

COMPUTER CRIME

Alabama—The Computer Crime Act punishes offenses against intellectual property -- accessing, communicating, examining, modifying or destroying computer data without authorization. Unauthorized disclosure of data is a crime. Ala. Code 13A-8-101.

Alaska—"Property" in the criminal code includes "intangible personal property including data or information stored in a computer program, system, or network." Alaska Stat. sec. 11.81.900(b)(44).

Alas. Stat. sec. 11.46.200(a) was amended in 1984 to define the unauthorized use of computer *time* as "theft of services."

Arizona—State law defines types of crimes using computers and makes them punishable as felonies. Ariz. Rev. Stat. sec. 13-2301E. Also, 13-2316.

California—It is a crime "to intentionally access . . . any computer system or computer network for the purpose of devising or executing any scheme or artifice; to defraud or extort or obtain money, property or services with false or fraudulent intent, representations, or promises; or to maliciously access, alter, delete, damage, or destroy, any computer system, computer network, computer program or data." Cal. Penal Code sec. 502.

Publishing a Personal Identification Number (PIN), password, access code, debt card number, or bank account number is a crime. Penal Code sec. 484j.

Colorado—This law, similar to Florida's, creates a Class 3 misdemeanor for computer crimes. Colo. Rev. Stat. sec. 18-5.5-101.

Connecticut—Computer crime is a misdemeanor or a felony, depending on the dollar amount involved. Conn. Gen. Stat. Ann. sec. 53a-250.

Delaware—Accessing a computer system for defrauding or obtaining money or services is computer fraud, and intentionally accessing, altering, destroying or attempting to do so for an improper purpose is computer misuse, both felonies. Del. Code tit. 11, sec. 931 to 939.

Florida—It is a felony to commit offenses against intellectual property; against computer equipment or supplies; or against computer users. The law prohibits willful modification, destruction, and disclosure. Fla. Stat. Ann. sec. 815.01. [See 1984-85 book.]

Georgia—Accessing or attempting to access a computer system owned by the state or under state contract or owned by any business is punishable by a fine and up to 15 years. Ga. Code Ann. sec. 16-9-90.

Hawaii—Computer fraud is a felony or misdemeanor depending upon the amount of money or damages involved. Computer fraud includes accessing a system with intent to defraud or to obtain money, get credit information, or introduce false information. Also, to wrongfully damage or enhance the credit rating of any person is a crime. Unauthorized computer use is a separate crime. Haw. Rev. Stat. 708-890.

Idaho—The law distinguishes between accessing or altering information with fraudulent purposes (a felony) and access only (a misdemeanor). Session Laws of Idaho 1984, ch. 68, p. 129, adding Idaho Code sec. 18-22.

Illinois—Without the consent of the owner, it is illegal to alter a computer program, to access a system, or to obtain uses or benefits from it. There is a civil right of action for victims of computer crime. Ill. Rev. Stat. Ann. ch. 38, sec. 16-9, as amended in 1983.

Indiana—A person who knowingly alters a computer program or data that is part of a system commits the felony of computer tampering. A person who accesses a system without consent commits a misdemeanor. IC 35-43-1-4.

Iowa—The computer crime law was effective July 1, 1984. Iowa Code Ann. sec. 716A.

Kansas—"Willfully exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing or taking possession" are crimes, as well as using a computer to defraud or to obtain money fraudulently. Kans. Stat. sec. 21-3755.

Kentucky—Fraudulently accessing a system to defraud, to obtain money or services, or to alter, damage, or attempt to alter information is a felony. Access for the sole purpose of obtaining information is a misdemeanor. A person is guilty of "misuse of computer information" when he or she receives, conceals, or uses any proceeds from an act in violation of the law (or aids another in doing so). Ch. 210, Acts of 1984, adding Ky Rev. Stat. sec. 434.

Louisiana—Computer-related offenses are defined in La. Rev. Stat. 14:73.1 through 5.

Maryland—"No person shall intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software..." Personal home computers and dedicated computers are excluded. Md. Ann. Code Art. 27, sec. 146.

Massachusetts—"Property" in the larceny statute includes "electronically processed or stored data, either tangible or intangible [and] data while in transit." Mass. Gen. Laws Ann. ch. 266, sec. 30(2).

Michigan—Computer fraud is a crime. Mich. Comp. Laws Ann. sec. 752.791.

Minnesota—Whoever intentionally and without authority damages or alters computer media is subject to a fine, depending on the loss involved, and prison term. Minn. Stat. Ann. sec. 609.87.

Mississippi—Computer fraud is a crime, as well as intentionally denying an authorized user effective use of a system or disclosure or misuse of codes or passwords. Miss. Code Ann. sec. 97-45-1.

Missouri—It is a crime to tamper with intellectual property. Mo. Ann. Stat. sec. 569.093.

Montana—The criminal code prohibits unlawful use of a computer, and "property" as defined in the criminal code on theft includes "any tangible or intangible thing of value . . . electronic impulses, electronically processed or produced data." Mont. Code Ann. 45-6-310.

Nebraska—Unauthorized access or disruption of a computer system is a felony. Neb. Rev. Stat. sec. 28-1343.

Nevada—A person who without authority denies the use of a computer to a person who has the duty and the right to use it is guilty of a misdemeanor. Also, using a computer without authority, to get personal information on another or to enter false information about another person in order to alter a credit rating is a crime. Nev. Rev. Stat. sec. 205.473.

New Hampshire—Accessing, intercepting, or adding to computer data is a crime, unless the person believed that he had authority. N. H. Rev. Stat. Ann. sec. 638:16.

New Jersey—There is a civil liability for computer-related fraud (N.J. Rev. Stat. sec. 2A:38A-1) and criminal liability (N.J. Rev. Stat. sec. 2C:20-1).

New Mexico—Misuse of a computer is a felony. Computer Crimes Act of 1979. N.M. Stat. Ann. sec. 30-16A-1. [See 1981 book.]

New York—Intruding into a computer system with confidential medical or personal information is a crime. Also, tampering with computer data while trying to commit a felony is itself an offense, as well as making unauthorized duplications of data. The law permits the state to prosecute a person in another state who taps into a computer in New York without authorization. N.Y. Penal Law Art. 156.

North Carolina—This law punishes computer-related offenses, including physical damage to a unit, wrongfully accessing a computer or network, and altering or damaging computer software, and seeking to extort by use of a computer. N.C. Gen. Stat. 14-453.

North Dakota—Computer fraud by accessing, altering, damaging, destroying without authority with intent to defraud or deceive or control property or services is a Class B felony. Doing so without false pretense is a Class C felony. N.D. Cent. Code sec. 12.1-06.1-08.

Ohio—The criminal code was amended in 1982 to include computer media in the definition of stolen property. Ohio Rev. Code Ann. sec. 2901.01 and 2913.01.

Oklahoma—Like Pennsylvania's, this law, passed in 1984, distinguishes computer hacking (a misdemeanor) from fraudulent alteration of, or damage to, computer data (a felony). Okla. Stat. Ann. tit. 21, sec. 1951–1956.

Oregon—Two classes of computer fraud are defined, prohibiting unauthorized access to systems. Or. Rev. Stat. 164.377.

Pennsylvania—Accessing, altering, damaging, or destroying any computer, system, or data base with criminal intent is a third-degree felony. Tampering, where no greater crime occurs, is a misdemeanor. Pa. Stat. Ann. tit. 18, sec. 3933.

Rhode Island—Similar to California's law, R.I. Gen. Laws sec. 11-52-1.

South Carolina—The computer crime law defines "computer hacking." S.C. Code sec. 16-16-10.

South Dakota—The state's 1982 law was amended in 1984 to punish "computer hacking," including the use or disclosure of passwords without the consent of the owner. It also punishes wrongful access to computerized information, as well as altering or disclosing. S.D. Codified Laws Ann. sec. 43-43B-7.

Tennessee—The Computer Crimes Act of 1983 prohibits damaging or altering computers or computer data. Tenn. Code Ann. sec. 39-3-1404. [See 1984-85 book.]

Texas—It is a misdemeanor to use a computer or to gain access to it without consent when there is a computer security system in place; or to alter or damage a program or cause a system to malfunction. It is a felony if the loss exceeds $2500. Tex. Penal Code Ann. 33.01. It is a misdemeanor to disclose a secure password to another person. Legislative records are protected by Tex. Civ. Stat. Ann. art. 5429b.

Utah—The altering, damaging or wrongful access of computer records is punishable as a misdemeanor or felony. Utah Code Ann. sec. 76-6-701.

Virginia—Fraudulent use of a system as well as trespassing in a system so as to cause a malfunction, alter data, or affect a financial transaction, is prohibited. It is a crime to invade one's privacy by perusing medical, employment, salary, credit or other financial or personal data relating to another person and stored in a computer. Va. Code Ann. sec. 18.2-152.1, enacted in April 1984. [See 1984-85 book.]

Washington—The computer crime law was enacted in March 1984. Wash. Rev. Code Ann. sec. 9A.48.100.

Wisconsin—It is a crime to modify, destroy, access, take, or copy data, programs or supporting documentation in a computer. Wisc. Stat. Ann. sec. 943.70.

Wyoming—Passed in 1982 and amended the next year, the law defines crimes against intellectual property and makes it a crime wrongfully to access a system or to deny computer services to an authorized user. Another section prohibits crimes against equipment, including impairing government or public services. And a third section defines crimes against computer users. Wyo. Stat. sec. 6-3-501 through 504.

Federal law—It is a felony to trespass into a computer system and receive classified information with intent to injure the U.S.; and a misdemeanor to trespass and obtain information from a computer system, from across state lines. Trafficking in stolen computer passwords is a crime. 18 U.S.C. 1030, as amended by PL 99-474 in 1986.

P.L. 100-235, enacted in January 1988, requires each federal agency to provide mandatory training in computer security awareness. The National Bureau of Standards is to develop guidance and to set standards for encryption of data.