
A Review of Federal and State Privacy Laws

Presented by

BBBOnLine, Inc. and the Council of Better Business Bureaus, Inc.

Summary of Current Federal Privacy laws

Privacy law, especially since 1982, is largely a response to technological changes in computers, digitized networks, and the creation of new information products. The laws vary, but a common thread is protection against unauthorized use of the collected information and government access to private records.

Administrative Procedure Act. (5 U.S.C. §§ 551, 554-558) — Establishes detailed procedures for Federal agencies to follow during administrative hearings. The Act's provisions prescribe, for example, the means by which agencies must notify individuals of their rights and liabilities, and how agencies may collect, present, and evaluate evidence and other data in such hearings.

Cable Communications Policy Act (47 U.S.C. § 551) — Requires cable television operators to inform their subscribers annually about the nature of personal data collected, data disclosure practices, and subscriber rights to inspect and correct errors in such data. Prohibits a cable television company from using the cable system to collect personal information about its subscribers without their prior consent, and generally bars the cable operator from disclosing such data. Authorizes damage awards of at least \$1,000, and awards of punitive damages, costs, and attorneys' fees against cable television companies that violate the Act's subscriber privacy provisions.

Census Confidentiality Statute (13 U.S.C. § 9) — Prohibits any use of census data for other than the original statistical purpose. It also prohibits any disclosure of census data that would allow an individual to be identified, except to sworn officers and employees of the Census Bureau.

Children's Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501 et seq., 16 C.F.R. § 312) — Generally requires a web site directed at children under 13 years of age to obtain "verifiable parental consent" before collecting personal information online from children. The COPPA regulation defines the term "collects" to encompass providing a child with the ability to have an e-mail account or the ability to post to a chat room, bulletin board, or other online forum. COPPA also requires a covered Web site to disclose in a notice its online information collection and use practices with respect to children, and provide parents with the opportunity to review the personal information collected online from their children.

Also prohibits a governmental entity from obtaining personal subscriber data in a cable television company's possession absent a court order reflecting a judicial finding that the data sought is likely to reveal criminal activity. Subscribers must be notified and provided with an opportunity to contest the government's claims.

Communications Assistance for Law Enforcement (47 U.S.C. § 1001) —

Preserves law enforcement's ability to engage in lawful electronic surveillance in the face of new technological developments. Increases the protections against governmental intrusions into the privacy of electronic communications. Requires that the government obtain a court order before obtaining tracking information or location information about subscribers from mobile service providers and explicitly states that it does not limit the rights of subscribers to use encryption.

Computer Security Act (40 U.S.C. § 1441) — Protects data maintained in government computers and requires each Federal agency to provide mandatory training in computer security awareness.

Criminal Justice Information Systems (42 U.S.C. § 3789g) — Requires Federally-funded State and local criminal justice information systems to include information on the disposition of any arrest. Permits individuals to see, copy, and correct information about themselves in the system.

Customer Proprietary Network Information (47 U.S.C. § 222) — Restricts private sector access and use of customer data. Prohibits the disclosure of individualized customer data obtained for purposes of providing telecommunications service absent customer approval. Imposes restrictions on the use of such data in aggregate form.

Driver's Privacy Protection Act (18 U.S.C. § 2721) — Prohibits State Departments of Motor Vehicles (DMVs) from releasing "personal information" from drivers' licenses and motor vehicle registration records. Permits the release of the information to recipients who are using it for one or more specific statutory purposes, or where the subject of the record was furnished with an opportunity to limit the release of the information and did not do so. Penalizes the procurement of information from motor vehicle records for an unlawful purpose, or the making of a false representation to obtain such information from a DMV. Imposes a record keeping requirement on the resellers of such information. The Act does not interfere with the ability of states to enact laws furnishing greater privacy protection to their drivers and vehicle owners.

Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3) — Prohibits disclosure of information collected for federally-funded research and treatment of drug abuse and alcoholism. It also prohibits use of this information for any purpose outside of the research or treatment program, except in cases of medical emergency or where a court order has been issued. Such information is specifically protected from use against the subject of any criminal proceeding. Violators of this statute are subject to a fine.

Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.) — Prohibits persons from tampering with computers or accessing certain computerized records without authorization. The Act also prohibits providers of electronic communications services from disclosing the contents of stored communications. Usually requires that the customer be notified and given an opportunity to contest in court a government entity's request for access to electronic mail or other stored communications in the control of a provider of electronic communications services or remote computing services.

Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m) — Requires banks to make extensive disclosures to customers about specific electronic funds transfer (EFT) transactions, both at the time the transactions are made and in the form of periodic statements. Requires banks to notify customers, at the time they contract for EFT services, of their rights, liabilities, charges, procedures, etc., connected with the services, and of whom to contact if an unauthorized transfer is suspected. In the case of preauthorized periodic transfers – such as automatic bill paying – the bank must provide either positive or negative notice as to whether payments are being made on schedule.

Mandates detailed procedures for the resolution of any inaccuracies in customer accounts, and imposes liability on the bank for errors in the transmission or documentation of transfers. An individual who prevails in a civil action for a violation of the Act may recover actual damages sustained, a penalty of \$100 to \$1,000, attorney's fees and court costs, and in limited situations, treble damages. Criminal penalties may be imposed for deliberate violations of the Act. Numerous federal agencies also have administrative responsibility for enforcing the provisions of this Act.

Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.) — Prohibits employers from requiring a polygraph test as a condition of employment or using the results of such tests as the sole basis for disciplining employees or taking other adverse employment actions. Bars employers from publicly disclosing the results of polygraph tests unless disclosure is made to the government pursuant to a court order or for the purpose of providing the government with information on criminal conduct. Employers that violate the Act may be subject to a fine of up to \$10,000, injunctive relief such as employee reinstatements, and awards of damages, costs and attorneys' fees.

Employee Retirement Income Security Act (29 U.S.C. § 1025) — Requires employers to provide employees with access to information about their accrued retirement benefits.

Equal Credit Opportunity Act (15 U.S.C. § 1691, et. seq.) — Restricts inquiries into a credit applicant's sex, race, color, religion, or marital status. Prohibits the retention and preservation of certain information by creditors and requires the preservation of certain specified records relating to credit transactions. Regulates the manner in which information collected by creditors may be used in making decisions regarding the extension of credit.

Requires that, when credit is denied or revoked, the applicant must be either notified of the reasons for the decision or informed of his right to learn the reasons. In suits brought for violations of the Equal Credit Opportunity Act, successful plaintiffs may recover actual damages, punitive damages, attorneys' fees and court costs. Individual or class action suits may be maintained for administrative, injunctive or declaratory relief. Numerous Federal agencies also have enforcement responsibility for the provisions of this Act.

Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.) — Restricts collection and use of information that would result in employment discrimination on the basis of race, sex, religion, national origin and a variety of other characteristics.

Fair Credit Billing Act (15 U.S.C. § 1666) — Requires creditors, at the request of individual consumers, to investigate alleged billing errors and to provide documentary evidence of the individual's indebtedness. Prohibits creditors from taking action against individuals with respect to disputed debts while disputes are under investigation. Any creditor who fails to disclose required information is subject to a civil suit, with a minimum penalty of \$100 and a maximum penalty of \$1,000 on any individual credit transaction.

The Act also imposes criminal liability on any person who knowingly and willfully gives false or inaccurate information, fails to disclose required information, or otherwise violates any requirement imposed by the Act. Any such person is subject to a fine of \$5,000 and/or imprisonment for not more than one year.

Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) — Regulates the collection and use of personal data by credit reporting agencies. Requires that when a data broker is hired to prepare an “investigative consumer report” (an investigation into the consumer’s “character, general reputation, personal characteristics or mode of living” by means of interviews with friends, neighbors and associates), the request for information must be disclosed to the subject of the report, who is then entitled to learn the nature and scope of the inquiry requested.

Requires that, if a consumer report is used in any decision to deny credit, insurance or employment, the report user must tell the consumer the name and address of the reporting agency. Prohibits disclosure of consumer reports maintained by consumer reporting agencies without consent unless such disclosure is made for a legitimate business purpose or pursuant to a court order.

Requires reporting agencies to use procedures that will avoid reporting specified categories of obsolete information and to verify information in investigative consumer reports that are used more than once. Requires brokers to maintain security procedures, including procedures to verify the identity and stated purposes of recipients of consumer reports.

Individuals may sue credit reporting agencies or parties who obtain consumer reports for violations of the Act. Individuals may recover for actual damages suffered, as well as attorneys’ fees and court costs. Punitive damages or criminal penalties may also be imposed for willful violations of the Act. The Federal Trade Commission and other Federal agencies responsible for enforcing the provisions of this Act are also empowered to declare actions to be in violation of the applicable statute, issue cease and desist orders, and impose statutory penalties for noncompliance with agency orders.

Overhauling the Fair Credit Reporting Act is the **Consumer Credit Reporting Reform Act of 1996 (Reform Act)**. The Reform Act requires more frequent and fuller notification to consumers, disclosure of all information (rather than only the substance of the information) in the consumer’s file, and stricter reinvestigation when a consumer disputes the accuracy of information in his or her file. Imposes new restrictions on resellers of consumer credit reports and strengthens private enforcement rights for violations of the Fair Credit Reporting Act.

Fair Debt Collection Practices Act (15 U.S.C. § 1692 et seq.) — Limits the communications that debt collection agencies may make about the debtors whose accounts they are attempting to collect. Imposes liability on debt collectors for any actual damages sustained, as well as additional damages not to exceed \$1,000, court costs and attorneys' fees. Numerous Federal agencies also have administrative responsibility for enforcing the provisions of this Act.

Fair Housing Statute (42 U.S.C. §§ 3604, 3605) — Restricts the collection and use of information that would result in housing discrimination on the basis of race, sex, religion, national origin and a variety of other factors.

Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) — Permits a student or the parent of a minor student to inspect and challenge the accuracy and completeness of educational records which concern the student. Prohibits schools receiving public funds from using or disclosing the contents of a student's records without the consent of the student or of the parent of the minor student. Prohibits government access to personal data in educational records without a court order or lawfully issued subpoena, unless the government is seeking access to the records for a specified education-related purpose. Vests administrative enforcement of the Act in the Department of Education, and provides for termination of Federal funds if an institution violates the Act and compliance cannot be secured voluntarily.

Freedom of Information Act (5 U.S.C. § 552) (FOIA) — Provides individuals with access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information. Unlike those of the Privacy Act, FOIA procedures are available to non-resident foreign nationals.

Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 et seq) — Regulates the privacy of personally identifiable, nonpublic financial information disclosed to non-affiliated third parties by financial institutions. Requirements also attach to non-affiliated third parties to whom they transfer this information. Requires written or electronic notice of the categories of nonpublic personal information collected, categories of people to whom the information will be disclosed, consumer opt-out rights, and the company's confidentiality and security policies. Creates consumer right to opt out of disclosures to nonaffiliated parties before the disclosure occurs, subject to a long list of exceptions. Requires administrative, technical and physical safeguards to maintain the security, confidentiality, and integrity of the information. Generally prohibits disclosure of account numbers and access codes for credit, deposit or transaction accounts to a nonaffiliated party for marketing purposes.

Health Insurance Portability and Accountability Act (Pub. Law No. 104-191 §§ 262,264; 45 C.F.R. §§160-164) — Department of Health and Human Services regulation, which goes into effect in 2003, applies to individually identifiable health information that has been maintained or transmitted by a covered entity. Applies directly to three types of entities: health plans, health care providers, and health care clearinghouses. Also will require these covered entities to apply many of its provisions to their business associates, including contractors, third-party administrators, researchers, life insurance issuers and employers.

Requires health plans and health care providers to provide a written notice of how protected health information about an individual will be used, as well as an accounting of the circumstances surrounding certain disclosures of the information. Prohibits covered entities from disclosing covered information in a manner inconsistent with the notice.

Requires covered entities to obtain a patient's opt-in via "consent" form for both use and disclosure of protected information for treatment, payment or health care operations. Also requires covered entities to obtain a patient's more detailed opt in via an "authorization" form for both use and disclosure of protected information for purposes other than treatment, payment or health care operations.

Permits several forms of marketing and fundraising uses of protected information subject to receipt of written consent and subsequent provision of opportunity to opt out. Requires patient authorization for transfers of protected information for routine marketing by third parties.

Provides right to access, copy and amend the information in designated record sets, including in a business associate's records if not a duplicate of the information held by the provider or plan.

Health Research Data Statute (42 U.S.C. § 242m) — Prohibits disclosure of data collected by the National Centers for Health Services Research and for Health Statistics that would identify an individual in any way.

Mail Privacy Statute (39 U.S.C. § 3623) — Prohibits opening of mail without a search warrant or the addressee's consent.

Paperwork Reduction Act of 1980 (44 U.S.C. § 3501, et seq.) — Prohibits an agency from collecting information from the public if another agency has already collected the same information, or if the Office of Management and Budget does not believe the agency either needs or can make use of the information. Requires each Federal data collection form to explain why the information is being collected, how it is to be used, and whether the individual’s response is mandatory, required to obtain a benefit, or voluntary.

Privacy Act (5 U.S.C. § 552a) — Mandates that personal data be collected as much as possible directly from the record subject. Generally prohibits collection of information about an individual’s exercise of First Amendment rights (e.g., freedom of expression, assembly, and religion). Requires that when an agency requests information about an individual, it notify the individual of the agency’s authorization and purpose for collecting information, the extra-agency disclosures (“routine uses”) that may be made of the data collected, and the consequences to the individual for failing to provide the information. Requires agencies, on request, to provide individuals with access to records pertaining to them and an opportunity to correct or challenge the contents of the records.

Restricts Federal agencies from disclosing personal data except for publicly announced purposes, and requires agencies to (1) keep an accounting of extra-agency disclosures; to (2) instruct record management personnel in the requirements of the Act and the rules for its implementation; and (3) “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records.”

Places accountability for the handling of personal records on the record-keeping agency and its employees. Requires agencies to publish a detailed annual notice that describes each record system, the kind of information maintained, its sources, the policies governing management of the system, and the procedures for individuals to obtain access to records about themselves.

Allows an individual harmed by a violation of the Act to sue the agency for an injunction, damages, and court costs. It also provides criminal penalties — fines of up to \$5,000 — against employees who disclose records in violation of the Act.

Privacy Protection Act (42 U.S.C. § 2000aa) — Prohibits government agents from conducting unannounced searches of press offices and files if no one in the press office is suspected of a crime. Requires instead that the government request voluntary cooperation or subpoena the material sought, giving the holder of the material a chance to contest the action in court. Directs the U.S. Attorney General to issue guidelines for seeking evidence from other non-suspect third parties, with special consideration to such traditionally confidential relationships as doctor-patient and priest-penitent.

Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.) — Requires Federal agencies seeking access to private financial records either (1) to notify the subject of the purpose for which the records are sought and provide the subject with an opportunity to challenge the disclosure in court, or (2) to obtain a court order for direct access to the records if notice would allow the record subject to flee or destroy the evidence. Prohibits a Federal agency that has obtained access to an individual's financial records from disclosing the records to another agency without (1) notifying the individual and (2) obtaining certification from the receiving agency that the records are relevant to a legitimate law enforcement inquiry of the receiving agency. Where a government agency or a financial institution discloses records or information in violation of the Right to Financial Privacy Act, the agency or institution is liable to the customer for any actual damages sustained, a \$100 penalty, punitive damages for willful or intentional violations, court costs, and attorney's fees.

Tax Reform Act (26 U.S.C. §§ 6103, 6108, 7609) — Requires notice and opportunity-to-challenge procedures (similar to those of the Right to Financial Privacy Act) before the Internal Revenue Service may obtain access to certain institutional records about an individual in the hands of certain private record keepers. Strictly limits disclosure of tax returns and return information, and in some cases requires a court order for disclosures to law enforcement agencies for purposes unrelated to tax administration.

Telephone Consumer Protection Act (47 U.S.C. § 227) — Requires entities who use the telephone to solicit individuals, to provide such individuals with the ability to prevent future telephone solicitations. Requires those who engage in telephone solicitations to maintain and honor lists of individuals who request not to receive such solicitations for ten years. Prohibits unsolicited commercial telephone calls using an artificial or pre-recorded voice without consumer consent. Prohibits the sending of unsolicited advertisements to facsimile machines.

Video Privacy Protection Act (18 U.S.C. § 2710) — Affords users and purchasers of commercial videotapes rights similar to those of patrons of libraries. Prohibits videotape sale or rental companies from disclosing customer names and addresses, and the subject matter of their purchases or rentals for direct marketing use, unless the customers have been notified of their right to prohibit such disclosures. Restricts videotape companies from disclosing personal data about customers without customers' consent or court approval. Requires that subscribers be notified and provided with an opportunity to contest a data request prior to a judicial determination. Video companies that violate the Video Privacy Protection Act may be liable for damage awards of at least \$2500, punitive damages, costs and attorneys' fees.

Wiretap Statutes (18 U.S.C. § 2510, et seq.; 47 U.S.C. § 605) — Prohibits the use of eavesdropping technology and the interception of electronic mail, radio communications, data transmission and telephone calls without consent. The Federal Communications Commission also has a rule and tariff prescription prohibiting the recording of telephone conversations without notice or consent.

Summary of State Privacy Laws

Bank Records Statutes — Prohibit financial institutions from disclosing financial records of a customer to a third party without legal process or customer consent.

Cable Television Statutes — Permit subscribers to correct information or have their names deleted from data files maintained by cable operators. Prohibit disclosure of personal information collected by a cable operator unless the subscriber has had notice and has not objected to the disclosure.

Common Law Remedies — Provide redress for invasion of privacy (i.e., intrusions into places of affairs as to which an individual has a reasonable expectation of privacy), public disclosure of privacy facts, defamation (i.e., disclosures of inaccurate personal information), and breach of duty of confidentiality. Provide for money damages and, in some cases, nominal, special or punitive damages, and injunctive relief.

Computer Crime Statutes — Prohibit individuals from tampering with computers or accessing certain computerized records without authorization. Persons engaged in such conduct are subject to criminal penalties, civil damages or both.

Credit Reporting Statutes — Prohibit collection by creditors of information on race, religion, or sex. Restrict disclosure by credit reporting agencies of credit information to third parties.

Criminal Justice Information Statutes — Require law enforcement agencies to permit individuals to see, copy and correct information about themselves maintained in the criminal justice information systems. Require that criminal justice information be reported promptly, completely and in standard format. These statutes also have quality control requirements for computerized information systems and special requirements that arrest records indicate the disposition of the case. In addition, most of the State criminal justice information statutes require strict security measures to protect this information.

Employment Records Statutes — Prohibit employers from collecting information about a job applicant's race, sex, color, religion, national origin and other attributes. Allow individuals access to personnel records held by their employers.

Fair Information Practices Statutes — Limit the type of information that State governments can collect and maintain about individuals. Allow individuals to inspect and challenge information about them held by the State. Restrict the ability of State governments to disclose personal data to third parties.

Genetic Information — Limit use of genetic information for therapeutic or diagnostic purposes. Prohibit use of information as a condition to determine eligibility for health, disability, life or other forms of insurance.

Insurance Records Statutes — Require insurers to provide general information about their personal data practices to applicants and policyholders, with further information available upon request. Require them to notify applicants about the collection and disclosure of personal data, and to specify when information is requested solely for marketing or research purposes. Restrict the use of “pretext interviews” (in which the identity or purpose of the interviewer is misrepresented) and require specific consent forms to be used for the collection of information that requires authorization from an individual. Permit individuals who are denied insurance to learn the specific reasons for such denial and to obtain access to the information used in refusing coverage.

Applicants or policy holders also may obtain access to non-privileged personal information about them, and may propose that such information be corrected, amended or deleted. Except where such disclosure is permitted by law, these statutes prohibit insurers from disclosing (without the individual’s consent) information they collect on individuals.

Media Shield Statutes — Permit journalists to refuse to identify the sources of information received in the course of professional employment.

Medical Records Statutes — Allow individuals to have access to their medical records. Limit the use and disclosure of medical or mental health records.

Polygraph Test Statutes — Restrict the use of mandatory polygraph tests as a condition for employment.

Privilege Statutes — Limit the introduction into legal proceedings of personal information maintained by professionals such as doctors, psychotherapists, attorneys, clergy and accountants, concerning individuals with whom they have a professional relationship.

School Records Statutes — Permit students and their parents to inspect and challenge the accuracy and completeness of school records. Limit the ability of schools to disclose information from school records to third parties. (See citations.)

Stored Wire Communications Statutes — Require notice to subscribers before the government can access stored wire communications.

Tax Return Statutes — Prohibit disclosure by the government of State tax returns and return information.

Telephone/Facsimile Solicitation — Restricts home telephone solicitations from using recorded messages; limits unsolicited fax advertisements.

Uniform Commercial Code — Encourages financial institutions to disclose to their customers in a timely fashion the record of all transactions by holding the financial institution responsible for any errors until after the customer is informed of the bank's version of what has occurred.

Video Privacy Statutes — Restrict videotape sales or rental companies from disclosing personal data about customers without their consent.

Wiretap Statutes — Restrict electronic eavesdropping and interception of communications by wire or radio. Some states also have tariff prescriptions requiring common carriers operating within their jurisdictions to terminate subscribers who record telephone conversations without notice or consent.