



PRIVACY LAWS

SYRACUSE UNIVERSITY
School of Information Studies

PRIVACY PROTECTION APPROACHES

Government enforcement approach

Self-regulation approach

Co-regulation



<https://goo.gl/7bn2FG>



<https://goo.gl/ofVBuh>

U.S. PRIVACY LAWS, PART I

Year	Law	Objective
1970	Fair Credit Reporting Act	Promotes the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies
1974	Privacy Act	Governs the collection, maintenance, use, and dissemination of personally identifiable information that is maintained by federal agencies
1978	Right to Financial Privacy Act	Gives the customers of financial institutions the right to some level of privacy from government searches
1986	Electronic Communications Privacy Act	Restricts the government use of wire taps in transmissions of electronic data by computer
1999	Gramm-Leach-Bliley Act	Protects individuals personal financial information held by financial institutions

U.S. PRIVACY LAWS, PART II

Year	Law	Objective
1988	Video Privacy Protection Act	Prohibits “video providers” from the disclosure of rental information
1996	Health Insurance Portability and Accountability Act (HIPAA)	Prohibits the use and disclosure of individual health information that is not authorized or required
1998	Children’s Online Privacy Protection Act	Governs the collection, maintenance, use, and dissemination of personally identifiable information that is maintained by federal agencies
2001	Patriot Act	Streamlines federal surveillance guidelines to simplify tracking possible terrorists

PRIVACY AND U.S. LAW: PRIVACY ACT OF 1974

Protects records that can be retrieved by personal identifiers such as a name, Social Security number, or other identifying number or symbol. An individual is entitled to access to his or her records and request correction of these records, if applicable.

Prohibits disclosure of records without the written consent of the individual(s) to whom the records pertain, unless one of the 12 disclosure exceptions enumerated in the act applies.

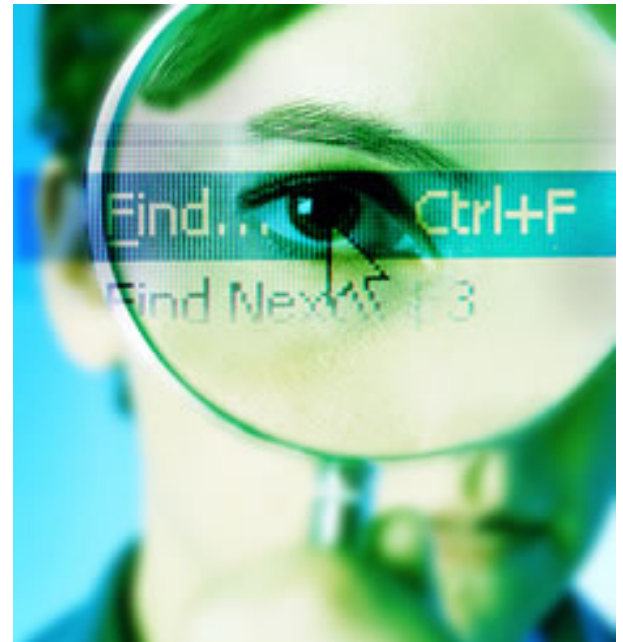
Requires an agency to publish in the Federal Register a system of records notice for every collection of records from which information can be retrieved by a personal identifier.

Binds only federal agencies and covers only records in the possession and control of federal agencies.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

Requires operators of websites and online services that collect information from children under 13 to:

- Post a privacy policy on the home page of the website and link to the privacy policy on every page where personal information is collected.
- Provide notice about the site's information-collection practices to parents, and obtain verifiable parental consent before collecting personal information from children.
- Give parents a choice as to whether their child's personal information will be disclosed to third parties.
- Provide parents access to their child's personal information and the opportunity to delete the child's personal information



PRIVACY AND YOUTH: STUDENT DATA PRINCIPLES

10. Any educational institution with the authority to collect and maintain student personal information should
- a. have a **system of governance** that designates rules, procedures, and the individual or group responsible for decision-making regarding data collection, use, access, sharing, and security, and use of online educational programs;
 - b. have a policy for **notification of any misuse or breach** of information and available remedies;
 - c. maintain a **security process** that follows widely accepted industry best practices;
 - d. provide a designated place or contact where **students and families can go to learn of their rights** and have their questions about student data collection, use, and security answered.

A coalition of educational organizations. Student data principles. www.studentdataprinciples.org

ECPA-RELATED LAWSUITS

Amazon and Alexa: The plaintiff alleged that the software Alexa allowed Amazon to intercept and access user personal information.

AOL vs. Cyber Promotions: Cyber Promotions claimed First Amendment rights to send large amounts of unsolicited e-mail via AOL.

DoubleClick: Allegedly used cookies to collect personal information from web users without their consent and then sold that information at a profit.

PRIVACY AND GOVERNMENT AGENCIES: COLLISION OF PRIVACY AND SECURITY

ECPA: Communications that remain on a third party's server for longer than 180 days are considered abandoned and lose any expectation of privacy (e.g., Google e-mail)

National Security Agency (NSA): Surveillance to find threats to national security

Smartphones and any GPS-enabled devices as tracking devices

Drug Enforcement Administration (DEA): Hemisphere, AT&T database combed to find links between burner phones and drug dealers