IAPP Information Privacy Certification

Glossary of Common Privacy Terminology

Access

Access is one of the fair information practices. Individuals must be able to find out what personal information a company has on file about them and how the information is being used. Individuals must be able to correct erroneous information in such records.

Ad blocker

Software used on a personal computer to prevent advertisements from being displayed in a web browser. An ad blocker can help web pages load faster and prevent ad networks from tracking users.

Adequacy

As used in EU Data Protection Directive, adequacy refers to the existence of a legal regime in another country that provides sufficient protection for personal information. In other words, a country will be deemed "adequate" if its laws afford individuals rights that are similar to those afforded by the EU Data Protection Directive. If a country offers adequate protection, then data transfers from the EU to that country may occur without any further limitations. This concept has been expanded to encompass other types of data transfer mechanisms. For example, the U.S. Safe Harbor provides an adequate level of protection, so companies that are in the Safe Harbor may transfer data from the EU to the US. Similarly, the EU Model Contracts provide an adqeuate level of protection, so data may be transferred from the EU to any country, if the recipient has executed a Model Contract.

Adequate country

A country that has been deemed adequate by EU authorities (see *adequacy*). Data transfers from Europe to countries deemed adequate can occur without restriction. The only countries recognized as adequate in 2002 were Switzerland, Hungary, and Canada. Argentina was recognized as an adequate country in 2003. The US has not been deemed adequate because it does not have a comprehensive data protection regime. Transfers to the U.S. can occur within the Safe Harbor framework or by use of another authorization mechanism.

Adequate notice

A statement that notifies an individual that personally identifiable data are being collected and fully describes the purpose of collection as well as any intended use, disclosure and retention of the personal data. This notice will be adequate if the information provided is appropriate given the facts and circumstances of the notice.

Affiliate

An entity that controls, is controlled by, or is under common control or ownership with the entity that is the subject of the privacy notice. Affiliates include, for example, the entity's sister companies, parent or subsidiaries.

Affirmative consent

A customer's agreement, through opt-in, to receive certain types of communication.

Affiliate programs

Programs in which a company works with its affiliates to provide offers to customers of one or more of the affiliates.

Aggregate information

Complied or statistical information that is not personally identifiable. Examples of aggregate information include, but are not limited to, demographics, domain names, and website traffic counts.

Anonymity

Personal information that cannot be identified to any individual by the recipient.

Anonymizer

A service that enables anonymous web surfing by acting as an intermediary. An anonymizer service prevents a website from seeing your IP address or planting cookies on your computer.

Anonymizing the data

The act of removing personal identifiers from data; converting personally identifiable information to aggregate data.

Australian SPAM act

The SPAM Act of 2003 is intended to restrict the sending of electronic marketing without the consent of the individual. It applies to any commercial electronic message (e-marketing sent through e-mail, SMS, MMS, or instant message) that contains an offer to do business, sent within or from Australia, accessed in Australia, sent to someone present in Australia, or authorized for sending from Australia.

Authorization

The process by which an entity (such as a person or a computer system) determines whether another entity is who it claims to be. Authentication is different from *authorization.* Proper authentication ensures that a person is who he or she claims to be, but it says nothing about the access rights of the individual.

Automated decision making

When an individual is subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of personal information intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Banner ad

An advertisement on a web page, generally displayed at the top of the page. Banner ads are typically placed by ad networks for a fee; the subject of the banner ad may be completely unrelated to the web page on which it appears. Clicking a banner ad opens another website where there is more information about the product or service being advertised.

BBBOnline ©

The Better Business Bureau's online seal program that certifies eligible web sites for reliability and privacy. BBBOnline offers privacy standard-setting, verification, monitoring and review, consumer dispute resolution, and enforcement. is a corporate sponsor of BBBOnline.

Biometric identifier

A personal identifier that identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characters, voice prints and hand written signature).

Browser

A software application that enables end users to read HTML content (Web pages) on the Internet.

Business need

Employee-specific definition: Those functions or duties requiring access to employee personal data that are necessary to carry out business functions, to comply with applicable laws, or to administer its Human Resources functions. Examples of business needs include, but are not limited to:

1. Administration of workforce such as employee records maintenance, ranking process, wage/stock option planning, training administration, transfer, employment terminations, etc. ;
2. Operational requirements such as headcount planning and reporting and expense management;
3. A requirement by law (statute, regulation or court ruling) or contract, to which the individual is a party; a response to administrative or judicial process including a subpoena or search warrant;
4. Cooperation with governmental agencies or law enforcement, to the extent allowed or required by local law; and,
5. An emergency, which is believed to pose a risk of harm to person, property, or the business interest of the company.

Customer-specific definition: The use of customer data and/or the processing of customer data to support a company's ongoing relationship with the customer. Examples of business needs are:

1. Complete an order transaction;
2. Fulfill an information request from a customer;
3. Provide services, support or product updates;
4. Send marketing communications (when the customer has given explicit permission to do so);
5. A requirement by law (statute and regulation) or by a contract to which the individual is a party; a response to administrative or judicial process including a subpoena or search warrant; and,
6. An emergency which is believed to threaten risk of harm to person or property: the realization of a legitimate serious interest of which overbalances the individuals' right of privacy.

California Data Security Law (SB 1386)

A California law that requires entities to report promptly security breaches that compromise the personal information of any California resident to those residents.

CAN-SPAM Act of 2003

Full name: Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003 (CAN-SPAM).
A U.S. Federal law that regulates commercial e-mail. The law requires senders of commercial email to include certain types of notices in the email and to honor opt out requests. . The Federal Trade Commission has promulgated regulations for CAN SPAM compliance.

Customer Contact management (CCM)

Activities aimed at managing communications to customers to maximize their value to the company.

Chief Privacy Officer (CPO)

An official charged with ensuring that an organization develops and adheres to a privacy policy. This person, appointed by a designated approving authority, oversees employees who have access to and responsibility for the organization's privacy infrastructure.

Children's Online Privacy Protection Act of 1998 (COPPA)

Enacted in 1998, COPPA is a US Federal law that requires website operators tha target children under the age of 13 to post a privacy policy detailing any personally identifiable information collected from those children. These operators must generally obtain verifiable parental consent before collecting, using, or disclosing personal information from children under the age of 13.

Choice

An individual's ability to determine whether or how personal information collected from him or her may be used or disclosed by the entity that collected the information. Also: The ability of an individual to limit certain uses of his or her personal ifnormation. For example, an individual may have choice about whether to permit a company to contact the individual or share the individual's data with third parties

ClD

See*: Customer information database.*

CKM

See: *Customer knowledge management.*

Clear GIF

See: *Web beacon.*

Commercial contact

Contact made with the intent to sell or promote a product or service.

Confidential information

Individual information that may include national id number, home address and phone number information as well as salary information, job grade and job ranking information.

Confidentiality

The obligation of an individual, organization or business to protect personal information and not misuse or wrongfully disclose that information.

Collection

The process of obtaining personal information from either the individual directly, such as a web form or a registration form, or from another party, such as a business partner.

Consent

This privacy requirement is one of the fair information practices. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice (see above) about the use or disclosure of his or her information, consent is the individuals' way of giving permission for the use or disclosure. Consent may be affirmative (*e.g.*, opt in) or implied (*e.g.*, the individual didn't opt out.)

(a) Explicit Consent: A requirement that an individual "signifies" his or her agreement with a data controller by some active communication between the parties. According to the EU Data Protection Directive, explicit consent is required for processing of sensitive information. Further, data controllers cannot infer consent from non-response to a communication.

(b) Implicit Consent: Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Consumer

A subset of individuals who is a user or a potential user for retail and online products and services. Generally a consumer purchases a single product or service. May be used interchangeably with "customer" in many industries.

Cookies

Small text files stored on a client machine and later retrieved by a web server on a client machine. They allow the server to keep track of the browsers' activities, and connect individual web requests into something like a session. Cookies can also be used to prevent users from having to be authorized for every password protected page they access during a session by recording that they have successfully supplied their user name and password already. Since cookies are usually stored on a PC's hard disk, they are not usually portable. Cryptic or encrypted cookies with an unclear purpose, and which are set without the user's knowledge, alarm Internet privacy advocates. They may also violate data protection laws.

(a) Cookie buster: A third-party cookie is placed by an ad network or an Internet marketing company, not by the visited site.

(b) Cookie, downgraded: A persistent cookie that is deleted when the browsing session ends or the cookie expires, whichever comes first.

(c) Cookie, leashed: A cookie that is only sent on request to download first-party content. When requests are made for third-party content, these cookies are suppressed - that is, they are not sent

(d) Cookie, third-party: A third-party cookie is placed by an ad network or an Internet marketing company, not by the visited site.

COPPA

See: *Children's Online Privacy Protection Act.*

CPO

See: *Chief Privacy Officer*

CRM

See: *Customer relationship management.*

Customer

An individually identified or identifiable profile, which contains, at minimum, first name, last name, and at least one of: e-mail address, street address, or phone number. A customer can have multiple *personas* (e.g. personal or professional) and/or profiles. These personas/profiles may or may not be linked.

Customer Identification Database (CID)

A corporate database that assigns a unique identifier to each customer to help track that customer and protect customer privacy. CID-Person manages customer privacy contact permissions across the enterprise.

Customer Knowledge Management (CKM)

Activities related to managing customer information, from collection to dissemination, to maximize the value of that information to the company.

Customer relationship management (CRM)

Activities related to managing the customer relationship to give the customer a positive experience and to develop a dialogue with the customer to learn how to better meet customer needs.

Data commissioner

Government official that runs a data protection office and that is charged with enforcing a country's data protection laws.

Data controller

A controller is any person who makes decisions with regard to the processing of personal data, including decisions about the *purposes* for which the personal data are processed and the *manner* in which the personal data are processed. The EU directive defines a data controller as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law."

Data exporter

The company based in the EU which transmits the personal information out of the European Union.

Data importer

The company based outside the EU that receives the personal information.

Data lifecycle

The period from which an organization acquires personal information to the time when the information is removed from the organization. Components of the life cycle include: collection, storage, use, sharing and destruction.

Data processor

A data processor is a person who processes the data on behalf of the data controller, but who is not an employee of the data controller. A data processor is defined by the EU directive as: "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

Data protection

The management of personal information. In the United States, "privacy" is the term that is used in policies, laws and regulations. However, in the European Union and other countries, the term "data protection" often identifies privacy-related laws and regulations.

Data protection authority

See: *Data commissioner*.

Data protection legislation

Any national law that provides privacy protection by generally regulating the collection, storage and use of personal data within the country. The EU Directive required each member state to enact its own data protection legislation based on the model in the Directive.

Data protection office

See also: *Data protection authority, Data commissioner.*

Government agency that enforces data protection legislation. According to the EU directive: "Each member state shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the member states pursuant to this directive. These authorities shall act with complete independence in exercising the functions entrusted to them. Consultation when drawing up administrative measures or regulations relating to the processing of personal data. Each authority has investigative powers necessary for the performance of its supervisory duties, power to engage in legal proceedings in case of violations. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person."

Data quality

The quality of data is judged by four criteria: Does it meet the business needs? Is it accurate, complete, and recent? Data is of an appropriate qualify if these criteria are satisfied for a particular application.

Data standards

Standard method to store data to easily share among databases. CKM data standards contain the foundation block, which is basic customer information, and the library block, which is optional marketing-related information.

Data subject

Term used in some data protection legislation to describe an individual who is the subject of a personal data record.

Data subject's consent

As defined by the EU directive: "…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Data subject access

The right of individuals to access any of their personal data held by a data controller.

Deceptive trade practices

Law within the U.S. that deals with corporate entities who mislead or misrepresent products or services to consumers and customers. These practices are regulated by the Federal Trade Commission at the federal level and typically by the Attorney General's Office of Consumer Protection at the state level. These laws typically provide both for enforcement by the government to stop the practice and individual actions for damages brought by consumers who are hurt by the practices.

De-duplication / De-dupe

When similar files are compared to eliminate duplicates, as in customer records.

Destruction

A phase of the data lifecycle that pertains to how a company removes or destroys an individual's personal information.

Digital certificate

A specially formatted block of data that contains a public key and the name of its owner thereby binding the identity of the owner (or some other attribute) to a public/private key pair. The certificate also carries the digital signature of a trusted third party in order to authenticate it.

Digital signature

The process used to verify to the person receiving the information through an electronic transmission ("the receiver") that the person sending the information ("the transmitter") is who he or she purports to be and that the message has not changed from the time it was transmitted. In a digital signature, there is a data value generated by a public key algorithm based on the contents of a block of data and a private key, yielding an individual checksum that verifies the identity of the signer and the integrity of the data that is signed.

Directive

See: *EU directive.*

Directive for data protection in telecom sector 2002/58 EC

This EU directive defines in greater detail the impacts of data protection on the telecom sector, which includes the Internet. Under the new directive, electronic communication by automated means has to be formally opted in, unless there is an existing relationship. This required opt-in applies to all electronic communications.

Disclosure

The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. Disclosure is often used interchangeably with the terms "sharing" and "onward transfer".

Dispute resolution

The response to a valid complaint or grievance, or the action taken to correct faulty information, or to make amends for harm or inconvenience caused to an individual.

Domain name

The explicit name used by a company, individual or organization to provide access to a given Website.

Do-not-call Registry (DNC Registry)

The DNC Registry is a list of US individual who have indicated that they do not wish to receive unsolicited commercial telemarketing calls. U.S. laws generally prohibits companies from making unsolicited telemarketing calls to these individuals.

E-business (electronic business)

Conducting business functions on the Internet.

EEA

See: *European economic area.*

E-mail initiator

The party who causes an e-mail to be sent and whose content is its primary purpose, regardless of sender. US CAN-SPAM regulations give opt-out responsibilities to the initiator, whereas in the past, the industry had attributed them to the sender.

E-mail marketing

Using e-mail as a marketing, promotional, and sales communication vehicle to customers

E-mail vendor

A third-party vendor engaged to send e-mail marketing campaigns or messages.

Encryption

The process by which mathematical algorithms convert data into an unreadable format in order to enable secure transmission or storage.

Encryption software

Used as a security measure, encryption software scrambles data so that it is unreadable to interceptors without the appropriate descrambling information.

Enterprise Privacy Authorization Language (EPAL)

A specification produced by IBM and submitted to the World Wide Web Consortium in 2003. EPAL is a "formal language for writing enterprise privacy policies to govern data handling practices in IT systems".

Ethernet adaptor address

This is the personal name of the Ethernet card in one's computer. Ethernet is a commonly used networking technology.

EU Data Protection Directive

There are several directives dealing with personal data usage, but the most important is the generic one approved in 1995 (95/46EC), protecting individuals' privacy and personal data use. This was followed in 1997 by a more specific directive for the telecom sector (9766/EC), which was updated in mid-2002 by the European institutions to adapt it to new technologies and business practices. See europa.eu.int/comm/internal_market/privacy/index_en.htm.

EU Directive

Directive 1995 (95/46EC), protecting individuals' privacy and personal data use. The EU Directive was adopted in 1995 and became effective in 1998. The Directive recognizes the European view that privacy is a fundamental human right, and establishes a general comprehensive legal framework that is aimed at protecting individuals and promoting individual choice regarding the processing of personal data. The Directive imposes an onerous set of requirements on any person that collects or processes data pertaining to individuals in their personal or professional capacity. It is based on a set of data protection principles, which include the legitimate basis, purpose limitation, data quality, proportionality, and transparency principles, data security and confidentiality, data subjects' rights of access, rectification, deletion, and objection, restrictions on onwards transfers, additional protection where special categories of data and direct marketing are involved, and a prohibition on automated individual decisions. The Directive applies to all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to any employer. The Directive's key provisions impose serious restrictions on personal data processing, grant individual rights to "data subjects," and set forth specific procedural obligations, including notification to national authority. The Directive has been supplemented by additional directives including a specific directive for the telecom sector (9766/EC) and for e-commerce. [reference].

European Economic Area (EEA)

The EU plus Iceland, Norway, and Switzerland. Those countries are not official members of the European Union but are closely linked by economic relationship.

European Union (EU)

The European Union (EU) is an organization of European countries dedicated to increasing economic integration and strengthening cooperation among its members. The European Union was involved in the development of the Safe Harbor Principles that affect data flows from the European Union into the United States. As of March 2003 the member states include: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, and United Kingdom.

European works council

A body that is established for information and consultation between employers and workers in an international company that operates in Europe. It is required by law.

Fair information practices

The code of fair information practices is based on five principles, as set forth in Privacy Online: A Report to Congress, Federal Trade Commission, June 1998 (www.ftc.gov/reports/privacy3/fairinfo.htm):

1. Notice/Awareness: Customers should be given notice of an entity's information practices before any personal information is collected from them.

2. Choice/Consent: Customers should be given options as to how any personal information collected from them may be used.

3. Access/Participation: Customers should have the ability to access data about themselves and to contest the accuracy and completeness of that data.

4. Integrity/Security: Customer data should be accurate and secure. Security involves measures that protect against loss, unauthorized access, destruction, use, or disclosure of data.

5. Enforcement/Redress: There should be a mechanism in place to ensure compliance with the core fair information practice principles, and to give customers a method for addressing compliance violations.

Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) in the United States enforces a variety of federal antitrust and consumer protection laws, including the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and the Safe Harbor Principles. The Commission seeks to ensure that the nation's markets function competitively, and are vigorous, efficient, and free of undue restrictions. The Commission also works to enhance the smooth operation of the marketplace by eliminating acts or practices that are unfair or deceptive.

Financial Services Modernization Act

See: *Gramm-Leach Bliley Act (GLBA)*

Firewall

A software and/or hardware device to control access to a computer on a local area network from outside computers on the Internet.

Form

A document that contains blank fields into which users can enter data.

General Data Protection Directive 95/46 EC

This enforced directive defines the overall concept of data protection in the EU. Under this directive, individual personal data has to be collected openly and fairly with a clear explanation of the purpose for its collection.

Gramm-Leach Bliley Act (GLBA)

Also known as: The Financial Services Modernization Act of 1999. A U.S. Federal law that provided for sweeping changes in the financial services industry, allowing the creation of new financial services holding companies that could offer a full range of financial products and eliminating legal barriers to affiliations among banks, securities firms, insurance companies and other financial services companies. Title V of GLBA also included comprehensive privacy and security requirements, which have been expanded by regulations promulgated by the Federal Trade Commission and the Federal Banking Regulatory Agencies. It regulates the privacy of personal information collected, used or disclosed by financial institutions. The law requires that consumers be given an adequate privacy notice as well as the opportunity to opt out of any disclosure of personal information to non-affiliated third parties for marketing purposes. Financial institutions must also have appropriate information security programs.

Globally Unique Identifier (GUID)

A globally unique identifier used to identify a computer, a user, a file, etc. for tracking purposes. GUIDs are often represented as 32 hex numbers.

Health Insurance Portability and Accountability Act (HIPAA)

The Department of Health and Human Services has promulgated privacy and security regulations pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The goals of these rules are to ensure the privacy and security of health information at every level of the healthcare system These regulations impose significant obligations on healthcare providers, health plans and healthcare clearinghouses. HIPAA's Privacy Rule regulates the use and disclosure of protected health information (PHI). The Privacy Rule also affects financial institutions that process payments for healthcare services, other service providers that use protected health information to perform activities on behalf of covered entities, and employers that sponsor group health plans. While the Privacy Rule does not directly regulate employers, the new requirements do apply to "group health plans" that are sponsored by many employers. The Security Rule is composed of 18 standards and 36 implementation specifications, which together set the minimum floor for protecting PHI by all covered entities.

Host

Any computer on a network that is a repository for services available to other computers on the network.

Host name

The name of a computer that is attached to a network. The host name typically includes a computer name and the organization that the computer belongs to.

Hyperlink

An element in an electronic document that links to another place in the same document or to an entirely different document. Typically, the user clicks the hyperlink to open the linked document. Hyperlinks are the most essential ingredient of all hypertext systems, including the World Wide Web.

Hypertext mark-up language (HTML)

A defined set of codes that comprise the World Wide Web's standard computer language.

Hypertext transfer protocol (HTTP)

The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.

Identity Theft

The use of an individual's personally identifiable information (PDD) in order to fraudulently appropriate their identity.

Information (of the data subject)

In cases of collection of data from the data subject, the controller or representative must provide a data subject from whom data relating to himself/herself are collected with the following information:

(a) The identity of the controller and representative, if any;

(b) The purposes of the processing for which the data are intended; and,

(c) Any further information, such as the recipients or categories of recipients of the data,
    1. Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him or her in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Internet protocol (IP)

IP specifies the format of packets and the addressing scheme. Most networks combine IP with a higher-level protocol called transmission control protocol (TCP), which establishes a virtual connection between a destination and a source.

IP address

This address is a unique string of numbers that identifies a computer on the Internet or on a TCP/IP network. The IP address is expressed in four groups of up to three numbers, separated by periods. For example: 123.123.23.2.

(a) Dynamic: An IP address that is assigned temporarily whenever a device logs on, or dials up, to a network or an Internet service provider. The IP address may be different each time the device connects.

(b) Static: And IP address that does not change whenever a device logs on, or dials up, to a network or an Internet service provider. It is permanently assigned to one computer or device.

Isolation

Isolation is intended to cancel all enterprise contact with a customer and prevent any new contact. It is a designation made by the privacy team only, and in very rare instances, such as threat of legal action, death of the customer, or requested deletion of all records. Isolation status is not directly visible to the customer and requires special handling.

List suppression

The process of stopping communications to customers who should not receive communications by flagging the records relating to those customers so they can be removed from the target list.

Log files

A record of activity that stores and displays information not explicitly given by the user. Examples of such information are: date, time, IP address, sites accessed, HTTP status, bytes sent, and bytes received.

Member state

In EU documents, this term refers to a country that is a full member of the European Union. There were 15 in 2002: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. Norway, Iceland, Switzerland, and the Channel Islands are *not* part of the EU, as of July 2003.

No opt

A company or entity that does not offer opt-in or opt-out as choices to the end users most commonly, because they do not use personally identifiable information (PII) beyond the original purpose for collecting the information.

Notice

A written description of an entity's practices with respect to its collection, use an disclosure of personal information. A privacy notice typically includes a description of what personal information the entity collects, how the entity uses the information, with whom it shares the information, whether the information is secured, and whether an individual has any choices as to how the entity uses the information.

Notification

Some EMEA countries are requiring that any database storing personal data or any processing of personal data should be registered with the local data protection office.

Opt-in

A consumer's expression of affirmative consent based upon a specific act of the consumer.

Opt-out

The consumer exercise of choice by affirmative requesting that a particular use of disclosure of data not occur.

P3P

See: *Platform for Privacy Preferences Project*

Password

A privat, unique series of letters and/or numbers that is created by an individual in order to gain access to an application, Website, system, device, or physical location.

Patriot Act (USA-PATRIOT)

Full name: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA-PATRIOT).
A US Federal law that was enacted in the wake of the September 11th terrorist acts. This omnibus law contains separate titles that enhance domestic security against terrorism (Title I), provide for additional surveillance authority (Title II) and increased border protection and immigration requirements (Title IV), remove obstacles to law enforcement investigations of terrorism (Title V), create the September 11 relief fund (Title VI), increase information sharing and intelligence for critical infrastructure protection and counter-terrorism (Titles VII and IX), and establish additional criminal laws against terrorism (Title VIII). The law gives broad power to law enforcement agencies to compel production of private sector data for anti-terrorism purposes. It also imposes strict obligations on financial institutions to know their customers and to report certain types of transactions to the government. The Federal Banking Regulatory Agencies have promulgate many different types of regulations under this Act.

Personal information

Any information that (i) relates to an individual and (ii) identifies or can be used to identify the individual. Such information may include an individual's name, postal address, e-mail address, telephone number, Social Security number, or other unique identifier.

Personal Information Protection and Electronic Documents Act (PIPEDA)

Comprehensive data protection legislation enacted in Canada. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to "every organization" in respect to "personal information" that the organization collects, uses or discloses in the "course of commercial actives," regarding customer and employee information. Personal information is defined as information about an identifiable individual, but does not include the name, title, business address or telephone number of an employee of an organization. Commercial activity is defined as any particular transaction, act or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists. The Act requires organizations to adhere to ten standards regarding the information that they collect: (1) Accountability, (2) Identifying Purposes, (3) Consent, (4) Limiting Collection, (5) Limiting Use, Disclosure and Retention, (6) Accuracy, (7) Safeguards, (8) Openness, (9) Individual Access, and (10) Challenging Compliance. PIPEDA is enforced by the Canadian Federal Privacy Commissioner.

Personally Identifiable Information (PII)

Any information that can be traced to a particular individual. Usually a set of identifiable information is identified through an identification block of data, such as a name, mailing address, phone number, social security number, or e-mail address. Personal user preferences tracked by a website via a cookie are also considered personally identifiable when linked to other personally identifiable information provided by a user online.

Platform for Privacy Preferences Project (P3P)

A set of guidelines and standards, developed by the W3C consortium, which helps in the implementation of privacy-friendly applications. One of the earliest implementations added browser features that could be used to analyze privacy policies and which allowed users to control what personal information is revealed in a semi-automatic way.

Pretexting

The use of false pretenses, including fraudulent statements and impersonations, in order to obtain consumers' personal information, such as bank balances.

Pretty Good Privacy (PGP)

Widely used encryption software from PGP Security. The initials stand for Pretty Good Privacy.

Primary Use

Personal information used for the purpose as that which the information was originally collected.

Privacy

The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual's expectations. Also, the right of an individual to control the collection, use, and disclosure of personal information.

Privacy officer

See: *Chief Privacy Officer.*

Privacy policy

An organization's standard pertaining to the user information it collects and what is done with the information after it is collected.

Privacy seal program

A program, such as BBBOnline or TRUSTe, that certifies compliance with a set of standards of privacy protection. Websites display the program's seal to indicate that they adhere to these standards.

Privacy statement

An organization's communication regarding its privacy policies, such as what personal information is collected, how it will be used, with whom it will be shared, and whether one has the option to exercise control over how one's information is used. Privacy statements are frequently posted on websites.

Processing of personal data

Any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Processor

See: *Data processor*.

Profile information

Information that can be associated or linked with a unique individual. It may be any attribute, such as address, favorite color, or the car he or she drives.

Protocol

A set of formal rules that describe how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and the transmission and error detection and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, the terminal to computer dialogue, character sets, and sequencing of messages.

Proxy server

A server that sits between a client application, such as a web browser, and a real server (such as a web server on the Internet). The proxy server intercepts all requests to the web server to determine whether it can fulfill the requests itself. If not, it forwards the requests to the web server. In many corporate or institutional networks, all requests for web pages go through a proxy server. Proxy servers can dramatically improve performance for groups of users, because they save the results of all requests for a certain amount of time. Frequently requested pages can be loaded from the proxy server, which is faster than loading them over the Internet. Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of websites.

Recipient

Any person, public authority, agency, or organization to whom data is disclosed, whether a third-party or not; however, authorities that may receive data in the framework of a particular inquiry shall not be regarded as recipients.

Register

To create an official customer record that contains the personal information required to uniquely identify the customer, protect the customer's privacy, and contact the customer.

Relationship communications

Communication with the primary purpose to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender.

SB 1386

See: *California Data Security Law*.

Safe Harbor

The European Commission's Directive on Data Protection went into effect in October 1998, and prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of privacy protection, the United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation, while the European Union relies on comprehensive legislation that requires creation of government data protection agencies, registration of databases with those agencies, and, in some instances, approval before personal data processing may begin. As a result of these different privacy approaches, the directive could have significantly hampered the ability of US companies to engage in many trans-Atlantic transactions. In order to bridge these different privacy approaches and provide a streamlined means for US organizations to comply with the directive, the US Department of Commerce and the European Commission developed a "Safe Harbor" framework. The Safe Harbor - approved by the EU in 2001 - is an important way for US companies to avoid interruptions in business dealings with the EU or prosecution by European authorities under European privacy laws. Certifying to the Safe Harbor assures that EU organizations know that a company provides adequate privacy protection, as defined by the directive. Safe Harbor is a self-regulation concept that applies ONLY for and is not expandable to other companies. For more information, see: www.export.gov/safeharbor/.

Secure sockets layer (SSL)

A protocol designed by the Netscape Communications Corporation to provide encrypted communications on the Internet.

Security

The protection of information to prevent loss, unauthorized access or misuse. Also, the process of assessing threats and risks to information and the procedures and controls to protect it

Sender

The person or company who sends an e-mail.

Sensitive personal data/sensitive information

The 1998 EU Directive distinguishes between ordinary personal data, such as name, address, and telephone number, and sensitive personal data, such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. Under the act, the processing of such data is subject to stricter conditions.

Spam

A colloquial term that refers to unsolicited or, unwanted electronic mail. The term first emerged in the early 1990s when an immigration law firm, Cantor & Siegel, sent unsolicited mass email messages

SSL

See: Secure sockets layer.

Strong authentication

The strong authentication scheme adopted by the directory standard relies on the use of a public-key cryptosystem, whereby each user possesses two keys, one public and one private, the latter of which is known only to the user. Each of these keys may be used to encipher or decipher the user's authentication information, in a complementary fashion (i.e. if the information was enciphered with the private key, it must be deciphered with the public key, and vice versa). If a user's public key is held by the directory, it can be used to confirm the user's identity if the user submits authentication information encrypted using his or her private key.

Subscription

Subscription contact applies to customers who request (opt in/subscribe to) a newsletter or subscription, or receive a specific communication as agreed to in terms of a service contract. This permission only applies to the specific program requested by the customer. This contact permission is not tracked or stored in the master customer database known as CID, but must be tracked and stored in appropriate local or "host" database(s).

Suppression

Suppression is honoring existing customer opt-out requests, typically, by removing anyone from a database who has opted out before making any contact using that database. Most enterprises recognizes three levels of opt-out: unsubscribe, enterprise-wide general, and isolation.

Tracker GIF

See: *Web beacon.*

Transactional contact

Contact with the primary purpose to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender.

Transfer

Sending personal data cross-border or from one company to another, which is necessary for operation of the company or for providing a service to a customer.

Transparency

A standard that requires that the structure for processing Personally Identifiable Information ("PII") be in a fashion that is open and understandable to the individual whose data is being processed. It is a goal of the Fair Information Practices, which requires a company to inform users what Personally Identifiable Information ("PII") the company collects and how the data is used.

TRUSTe

An online privacy seal program that certifies eligible web sites and holds web sites to a baseline privacy standard. It serves as a key privacy watchdog organization that is the mediator for many US companies' privacy disputes. TRUSTe plays an important enforcement role in the dispute and resolution of privacy issues.

Trusted systems

A trusted system is a user environment in which every action is controlled by permissions. For example, a user can only print out a document or copy and paste sections if he has the appropriate permission.

Unsubscribe

The method by which a customer chooses to stop receiving a particular program-specific communication.

USA-PATRIOT

See: *Patriot act.*

Verifiable parental consent

This can take several forms, as long as they are reasonable efforts in light of available technology. For example, current acceptable means of obtaining verifiable parental consent include the use of a consent form that can be downloaded and printed so the parent can fill it out, sign it, and send it back by fax or mail; or credit card verification in which the card number is verified in the course of a transaction or by other reliable means. Also known as *prior verifiable parental consent.*

Web beacon

Also known as: *Web bug*. A graphic on a web page or in an e-mail message that is designed to monitor who is reading the web page or e-mail message. Web beacons are often invisible because they are typically only 1-by-1 pixel in size, with no color. Among the information collected is the IP address of the computer that the web beacon is sent to, the URL of the page the web beacon comes from, and the time it was viewed. Web beacons are also known as web bugs, 1-by-1 GIFs, invisible GIFs, and tracker GIFs.