Accountability
A fair information practices principle, it is the principle that a data controller should be accountable for complying with measures which give effect to the other principles.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F18, 21-22; IP11-12; US34-35; C39, 101, 122; E8; G9

Act Respecting the Protection of Personal Information in the Private Sector
A Québécois privacy law that, other than different terminology, is similar to PIPEDA, though at a province level. It came into force in 1994 and espouses three principles: (1) Every person who establishes a file on another person must have a serious and legitimate reason for doing so; (2) The person establishing the file may not deny the individual concerned access to the information contained in the file; (3) The person must also respect certain rules that are applicable to the collection, storage, use and communication of this information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F48-49, C35-37

Active Data Collection
When an end user deliberately provides information, typically through the use of web forms, text boxes, check boxes or radio buttons.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F128; IP203

Associated term(s): Passive Data Collection

Adequate Level of Protection
A label that the EU may apply to third-party countries who have committed to protect data through domestic law making or international commitments. Conferring of the label requires a proposal by the European Commission, an Article 29 Working Group Opinion, an opinion of the article 31 Management Committee, a right of scrutiny by the European Parliament and adoption by the European Commission.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F36-37; IP84-85; C24; E38, 175-178, 295

Associated term(s): Adequacy
Administrative Purpose
The use of personal information about an individual in Canada in a decision-making process that directly affects that individual.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C68

Adverse Action
Under the Fair Credit Reporting Act, the term “adverse action” is defined very broadly to include all business, credit and employment actions affecting consumers that can be considered to have a negative impact, such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer. Such an action requires that the decision maker furnish the recipient of the adverse action with a copy of the credit report leading to the adverse action.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP31; US60-61; C124

Alberta PIPA
A privacy law in the Canadian province of Alberta, similar to PIPEDA, that came into force in 2004. Unlike PIPEDA, these acts clearly apply to employee information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C31

American Institute of Certified Public Accountants
A U.S. professional organization of certified public accountants and co-creator of the WebTrust seal program.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP6; C61-62

Acronym(s): AICPA
Associated term(s): Canadian Institute of Chartered Accountants, Seal Programs, WebTrust
GLOSSARY OF PRIVACY TERMS

Americans with Disabilities Act
A U.S. law that bars discrimination against qualified individuals with disabilities.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP117, 133; US156, 160-162; 165
Acronym(s): ADA

Annual Independent Evaluations
Under FIMSA, U.S. agencies’ information security programs must be independently evaluated yearly. The independent auditor is selected by the agency's inspector general or the head of the agency. The audit is submitted to the Office of Management and Budget.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G76
Associated law(s): FISMA

Annual Reports
The requirement under the European Data Protection Directive that member state data protection authorities report on their activities at regular intervals.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E196, E204
Associated law(s): Data Protection Directive

Antidiscrimination Laws
Refers to the right of people to be treated equally.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US155-156, 159-161; E100

APEC Privacy Principles
A set of non-binding principles adopted by the Asia-Pacific Economic Cooperative (APEC) that mirror the OECD Fair Information Privacy Practices.
Application-Layer Attacks
Attacks that exploit flaws in the network applications installed on network servers. Such weaknesses exist in web browsers, e-mail server software, network routing software and other standard enterprise applications. Regularly applying patches and updates to applications may help prevent such attacks.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F102; IP192

Article 29 Working Party
A European Union organization that functions as an independent advisory body on data protection and privacy. While EU data protection laws are actually enforced by the national Data Protection Authorities of EU member states.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F39; IP84; US138; C110; E198-200; C110

Authentication
The process by which an entity (such as a person or computer system) determines whether another entity is who it claims to be. Authentication identified as an individual based on some credential; i.e. a password, biometrics, etc. 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.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F94-95, 124, 128; IP178; C59
Associated term(s): Authorization

Authorization
In the context of information security, it is process of determining if the end user is permitted to have access to the desired resource such as the information asset or the information system containing the asset. Authorization criteria may be based upon a variety of factors such as organizational role, level of security clearance, applicable law or a combination of factors. When effective, authentication validates that the entity requesting access is who or what it claims to be.

Association term(s): Authentication
Background Screening/Checks
Verifying an applicant’s ability to function in the working environment as well as assuring the safety and security of existing workers. Background checks range from checking a person’s educational background to checking on past criminal activity.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F39, 98; IP124; US158-164; E215; G158

Bank Secrecy Act, The
A U.S. federal law that requires U.S. financial institutions to record, retain and report certain financial transactions to the government to assist in the investigation of money laundering.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP74; US72-74; G26-29

Acronym(s): BSA
Associated term(s): Financial Record Keeping and Reporting Currency and Foreign Transactions Act of 1970

BC PIPA
A privacy law in the Canadian province of British Columbia, similar to PIPEDA, that came into force in 2004. Unlike PIPEDA, these acts clearly apply to employee information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C32

Associated law(s): PIPEDA

Behavioral Advertising
The act of tracking users’ online activities and then delivering ads or recommendations based upon the tracked activities.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F134; IP210-211; US22, 24; C45-47; E261-264

Acronym(s): OBA
Associated term(s): Online Behavioral Advertising, Behavioral Targeting
BINDING CORPORATE RULES
Legally binding internal corporate privacy rules for transferring personal information within a corporate group. BCRs are typically used by corporations that operate in multiple jurisdictions, and they are alternatives to the U.S.-EU Safe Harbor and Model Contract Clauses. BCRs must be approved by the EU data protection authorities of the member states in which the corporation operates.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F37; IP154; US25; E184-186
Acronym(s): BCR
Associated law(s): EU Data Protection Directive

BINDING SAFE PROCESSOR RULES
Self-regulatory principles (similar to Binding Corporate Rules) for processors that are applicable to customer personal data. Once a supplier’s BSPR are approved, a supplier gains “safe processor” status and its customers would be able to meet the EU Data Protection Directive’s requirements for international transfers in a similar manner as BCR allow. BSPR are currently being considered as a concept by the Article 29 Working Party and national authorities.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E274, E296
Acronym(s): BSPR
Associated term(s): Binding Corporate Rules

BIOMETRICS
Data concerning the intrinsic physical or behavioral characteristics of an individual. Examples include DNA, fingerprints, retina and iris patterns, voice, face, handwriting, keystroke technique and gait.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F95; E238
Associated term(s): Personal Information

BODILY PRIVACY
One of the four classes of privacy, along with information privacy, territorial privacy and communications privacy. It focuses on a person’s physical being and any invasion thereof. Such an invasion can take the form of genetic testing, drug testing or body cavity searches.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F2; IP2


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

Breach Disclosure
The requirement that a data controller notify regulators and victims of incidents affecting the confidentiality and security of personal data. It is a transparency mechanism highlights operational failures, this helps mitigate damage and aids in the understanding of causes of failure.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F108-111; IP69-70; US117-118; C60-61, C129; E42, E159-161; G101-103
Associated law(s): FCRA, GLBA, HIPPA, various U.S. state laws
Associated term(s): Breach notification

Bring Your Own Device
Use of employees’ own personal computing devices for work purposes.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US171-172
Acronym(s): BYOD
Associated term(s): Consumerization of information technology (COIT)

Bundesdatenschutzgesetz
A German national data protection law that including specific requirements for data services outsourcing agreements. The legislation contains ten specific requirements for outsourcing agreements: (1) Subject and duration of work; (2) the extent, type and purpose of data processing; (3) technical and organizational measures to be taken under section 9; (4) the rectification, erasure and blocking of data; (5) the processor's section 4 obligations, particularly with regard to monitoring; (6) rights regarding subcontracting; (7) the controller's monitoring rights; (8) the subcontractor's notification obligations; (9) the extent of the controller's authority to issue instructions to the processor; (10) the return and/or erasure of data by the processor at the conclusion of the work.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E292
GLOSSARY OF PRIVACY TERMS

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Caching
The saving of local copies of downloaded content, reducing the need to repeatedly download content. To protect privacy, pages that display personal information should be set to prohibit caching.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F117; IP201

California Investigative Consumer Reporting Agencies Act
A California state law that requires employers to notify applicants and employees of their intention to obtain and use a consumer report.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US163
Acronym(s): ICRAA

Canada’s Anti-Spam Legislation
Canadian anti-SPAM legislation applying to all forms of electronic messaging. It requires that when a commercial electronic message (CEM) is sent, consent, identification and unsubscribing requirements must be complied with. Typically, consent from the recipient must be obtained before a CEM is sent. There are, however, a number of exceptions to the need for consent.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C37-38
Acronym(s): CASL

Canadian Institute of Chartered Accountants
The Canadian Institute of Chartered Accountants (CICA), in partnership with the provincial and territorial institutes, is responsible for the functions that are critical to the success of the Canadian CA profession. CICA, pursuant to the 2006 Protocol, is entrusted with the responsibility for providing strategic leadership, co-ordination of common critical functions of strategic planning, protection of the public and ethics, education and qualification, standard setting and communications.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP6; C6, C61
Acronym(s): CICA
Canadian Organization for the Advancement of Computers in Health
A Canadian health informatics association whose mission is to promote health technology systems and the effective use of health information.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C105
Acronym(s): COACH

Canadian Standards Association
A non-profit standards organization that developed its own set of privacy principles and broke the OECD’s code into ten principles: (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; (10) Challenging Compliance. These ten principles would go on to be listed in PIPEDA.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F49; IP81; C18-19
Acronym(s): CSA
Associated term(s): CSA Privacy Principles

Case Law
Principles of law that have been established by judges in past decisions. When similar issues arise again, judges look to the past decisions as precedents and decide the new case in a manner that is consistent with past decisions.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP22; US3

Charter of Fundamental Rights
A treaty that consolidates human rights within the EU. The treaty states that everyone has a right to protect their personal data, that data must be processed for legitimate and specified purposes and that compliance is subject to control by an authority.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E13, E16, E20

Charter Rights
Rights created by the Canadian Charter of Rights and Freedoms. They are constitutional rights and thus are considered to be the most valued rights in Canada. The Charter of Rights and Freedoms was made part of the Canadian Constitution in 1982.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C8

**Chief Privacy Officer (Agency level)**
A position within an organization that is responsible for managing risks of privacy laws and policies. Within the U.S. government, this position was created under section 522(a) of the Consolidated Appropriations Act of 2005.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G69

Acronym(s): CPO

**Children’s Online Privacy Protection Act of 2000, The**
A U.S. federal law that applies to the operators of commercial websites and online services that are directed to children under the age of 13. It also applies to general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires these website operators: to post a privacy policy on the homepage of the website; provide notice about collection practices to parents; 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 and the opportunity to delete the child’s personal information and opt out of future collection or use of the information, and maintain the confidentiality, security and integrity of personal information collected from children.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F43, 126-127; IP46-49, 221-223; US107-11; C127-128; G19-23

Acronym(s): COPPA

Associated term(s): 15 U.S.C. §§ 6501-6508

**Choice**
An individual’s ability to determine whether or how their personal information may be used or disclosed by the entity that collected the information. Also, the ability of an individual to limit certain uses of their personal information. For example; an individual may have choice about whether to permit a company to contact them or share their data with third parties. Can be express or implied.

GLOSSARY OF PRIVACY TERMS

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F16; IP8; US6, 21; C62, 115, 121; E105-106
Associated term(s): Consent

Ciphertext
Encrypted (enciphered) data.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Associated term(s): NIST SP 800-21

Closed Circuit Television
Systems of cameras, monitors and recording equipment that are not used for broadcasting but are connected to a closed network by cables. CCTV is used primarily for video surveillance of premises.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F11; IP145; US168; C165; E228, 233-238
Acronym(s): CCTV
Associated term(s): Video Surveillance

Cloud Computing
The storage of information on the Internet. Although it is an evolving concept, definitions typically include on-demand accessibility, scalability, and secure access from almost any location. Cloud storage presents unique security risks.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F86, 139-141; E269

Collection Limitation
A fair information practices principle, it is the principle stating there should be limits to the collection of personal data, that any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F17, 20; IP11, 27, 98
GLOSSARY OF PRIVACY TERMS

Commercial Activity
Under PIPEDA, “commercial activity” means 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. Non-profit associations, unions and private schools are likely to be found to exist outside of this definition.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F49; IP81; US16; C27

Commercial Electronic Message
Any form of electronic messaging, including e-mail, SMS text messages and messages sent via social networking about which it would be reasonable to conclude its purpose is to encourage participation in a commercial activity. Examples include electronic messages that offer to purchase, sell, barter or lease products, goods, services, land or an interest or right in land; offers to provide a business, investment or gaming opportunity; advertises or promotes anything previously mentioned.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US96-97, 99; C37

Acronym(s): CEM

Common Law
Unwritten legal principles that have developed over time based on social customs and expectations.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US3, 23; G145

Communications Privacy
One of the four classes of privacy, along with information privacy, bodily privacy and territorial privacy. It encompasses protection of the means of correspondence, including postal mail, telephone conversations, electronic e-mail and other forms of communicative behavior and apparatus.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F2; IP2; US85-102; C3-4

Comprehensive Laws
GLOSSARY OF PRIVACY TERMS

Laws that govern the collection, use and dissemination of personal information in the public and private sectors.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F31-32; IP4-5; C4-5
Associated term(s):  Omnibus Laws  

Computer Forensics
The discipline of assessing and examining an information system for relevant clues even after it has been compromised by an exploit.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F107; IP193; C4-5

Computer Matching and Privacy Protection Act
Requires agencies that match data among agency systems granting financial benefits to publicly disclose that matching and explain its scope.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G54-55, 160

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

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F77

Confirmed Opt In
An e-mail approach where e-mail marketers send a confirmation e-mail requiring a response from the subscriber before the subscriber receives the actual marketing e-mail.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  US38
Associated term(s):  Double Opt In
GLOSSARY OF PRIVACY TERMS

Consent
This privacy requirement is one of the fair information practices. Individuals must be able to prevent the collection of their personal data, unless the disclosure is required by law. If an individual has choice (see Choice) 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; i.e., opt-in; or implied; i.e., the individual didn’t opt out. (1) 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. (2) Implicit Consent: Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F16; IP8-9; C28
Associated term(s): Choice

Consent Decree
A judgment entered by consent of the parties. Typically, the defendant agrees to stop alleged illegal activity and pay a fine, without admitting guilt or wrongdoing. This legal document is approved by a judge and formalizes an agreement reached between a federal or state agency and an adverse party.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP15-16; US4, 15-16
Associated term(s): FTC

Consumer Reporting Agency
Any person or entity that complies or evaluates personal information for the purpose of furnishing consumer reports to third parties for a fee.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US58-59
Acronym(s) CRAs
Associated term(s): Credit Reporting Agency

Convention 108
The first legally binding international instrument in the area of data protection. It requires signatories to take steps to ensure fundamental human rights with regard to the processing of personal information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP12; E9
Associated term(s): The Convention for the Protection of Individuals with Regard to Automatic
GLOSSARY OF PRIVACY TERMS

Processing of Personal Data

Cookie
A small text file stored on a client machine that may later be retrieved by a web server from the machine. Cookies allow web servers to keep track of the end user's browser activities, and connect individual web requests into 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. Cookies may be referred to as "first-party" (if they are placed by the website that is visited) or "third-party" (if they are placed by a party other than the visited website). Additionally, they may be referred to as "session cookies" if they are deleted when a session ends, or "persistent cookies" if they remain longer.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F38, 75, 135-137; IP215-217; C46; E274-275
Associated term(s): First-Party Cookie, Persistent Cookie, Session Cookie, Third-Party Cookie, Tracking Cookie, Web Cookie

Cookie Directive
Additions to the e-Privacy Directive where websites could allow users to opt out of cookies, such as by selecting a setting on their web browsers. Under the revision, member states are required to pass legislation that gives users the ability to opt in before cookies are placed on their computers.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F38, 75, 134; E263-264

Copland v. United Kingdom
A case in which the European Court of Human Rights held that monitoring an applicant's e-mail at work was contrary to Article 8 of the Convention on Human Rights.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E31

Co-regulatory Model
Emphasizes industry development of enforceable codes or standards for privacy and data protection

against the backdrop of legal requirements by the government. Co-regulation can exist under both comprehensive and sectoral models.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F30, 33-34; IP32
Associated term(s): Comprehensive Laws, Sectoral Laws, Self-regulatory Model, Technology Based Model

**Council of the European Union**
The main decision-making body of the EU, it has a central role in both political and legislative decisions. The council was established by the treaties of the 1950s, which laid the foundations for the EU.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E21, 25-27
Associated term(s): Council of Ministers

**Court of Justice of the European Union**
The Court of Justice is the judicial body of the EU that makes decisions on issues of EU law and enforces European decisions either in respect to actions taken by the European Commission against a member state or actions taken by individuals to enforce their rights under EU law. The court is the judicial body of the EU that makes decisions on issues of EU law and enforces European decisions. Based in Luxembourg, the Court was set up in 1951, and was originally named the Court of Justice of the European Communities. The court is frequently confused with the ECHR, which oversees human rights laws across Europe, including in many non-EU countries, and is not linked to the EU institutions.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E31-32

**Credit Freeze**
A consumer-initiated security measure which locks an individual’s data at consumer reporting agencies. Is used to prevent identity theft, as it disallows both reporting of data and issuance of new credit.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US123

**Credit Reporting Agency**
Under the Fair Credit Reporting Act, any organization that regularly engages in assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer

GLOSSARY OF PRIVACY TERMS

reports to third parties for a fee.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP29; US58-59; G159
Acronym(s): CRA
Associated term(s): Consumer reporting agency
Associated law(s): FCRA

Cross-site Scripting
Code injected by malicious web users into web pages viewed by other users.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F119; IP205
Acronym(s): XSS

Cryptography
The science or practice of hiding information, usually through its transformation. Common cryptographic functions include: encryption, decryption, digital signature and non-repudiation.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F97, 118; IP184
Associated term(s): Digital signature, encryption, non-repudiation, PKI

CSA Privacy Principles
The Canadian Standards Association (CSA) ten privacy principles are based on the OECD Guidelines and serve as the basis of Canada’s PIPEDA.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C18; G8-9
Associated term(s): Canadian Standards Association
Associated law(s): PIPEDA

Customer Access
A customer’s ability to access the personal information collected on them as well as review, correct or delete any incorrect information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F122-123; IP206, 243-244; US58

Customer Information
In contrast to employee information, customer information includes data relating to the clients of private-sector organizations, patients within the healthcare sector and the general public within the context of public-sector agencies that provide services.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F10
GLOSSARY OF PRIVACY TERMS

Data Breach
The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector. Breaches do not include good faith acquisitions of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector—provided the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F104-111; G98, 263
Associated term(s): Breach, Privacy Breach (Canadian)

Data Classification
A scheme that provides the basis for managing access to, and protection of, data assets.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US34

Data Controller
An entity that has the authority over the processing of personal information. This entity is the focus of most obligations under privacy and data protection laws. It controls the use of personal data by determining the purposes for its use and the manner in which the data will be processed. The data controller may be an individual or an organization that is legally treated as an individual, such as a corporation or partnership.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F8; IP13; E57-59, 288; G7
Associated term(s): Data Processor

Data Elements
The different types of personal information processed by data processors. Typical data elements include name, date of birth and numerical identifiers. Organizational data elements tied to both individuals as well as organizations include business addresses, business phone numbers, business e-mail addresses and related information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F5; IP7, 69; US49


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
**Data Matching**
An activity that involves comparing personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP103; C87-89

**Data Processing**
Any operation or set of operations which is performed on personal data, such as collecting; recording; organizing; storing; adapting or altering; retrieving; consulting; using; disclosing by transmission, dissemination or otherwise making the data available; aligning or combining data, or blocking, erasing or destroying data. Not limited to automatic means.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F35-36

Associated term(s): 
- Data Processor
- Processing
- Processor

**Data Processor**
An individual or organization that processes data on behalf of the data controller. Although they are often third-party providers, a data controller can also be a data processor.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F8; IP14; E57, 61-62, 288

Associated term(s): 
- Data Controller
- Processor

**Data Protection Authority**
An official or body that ensures compliance with data protection laws and investigates alleged breaches of the laws’ provisions.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F31; IP4; E39

Acronym(s): 
- DPA

**Data Protection Commissioner**
The person responsible for the enforcement and monitoring of compliance with data protection legislation, including Data Protection Acts. Commissioners are also responsible for investigating breaches of the laws.

legislation and prosecuting the senders of spam e-mails and text messages pursuant to SI 535/2003. Only one such prosecution has occurred to date. In the UK, this function is carried out by the Information Commissioner.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F33
Associated term(s): Data Protection Authority

Data Protection Directive

Several directives deal with personal data usage in the EU, but the most overarching is the general policy approved by the European Commission in 1995 (95/46EC) which protects individuals’ privacy and personal data use. The Directive was adopted in 1995, became effective in 1998 and protects individuals’ privacy and personal data use. 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 severe restrictions on personal data processing, grant individual rights to “data subjects” and set forth specific procedural obligations including notification to national authorities. This was followed in 1997 by a more specific directive for the telecom sector (97/66/EC), which was replaced in mid-2002 by the European institutions to adapt it to new technologies and business practices (2002/58/EC). The Directive has been supplemented by additional directives including a specific provision for e-commerce.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F18-19, 34-41; E37
Associated term(s): EU Data Protection Directive

Data Quality

A fair information practices principle, it is the principle that personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. The quality of data is judged by four criteria: Does it meet the business needs?; Is it accurate?; Is it complete?, and is it recent? Data is of an appropriate quality if these criteria are satisfied for a particular application.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F22; IP11; C19; E2; G70-71

GLOSSARY OF PRIVACY TERMS

Data Quality Act of 2000
Passed in response to the increased use of the Internet by U.S. federal agencies, the act was designed to ensure the quality of information released by agencies by establishing four major requirements: (1) Office of Management and Budget was to issue guidelines "ensuring and maximizing the quality, objectivity, utility and integrity" of disseminated information; (2) agencies must issue their own sets of information quality guidelines; (3) agencies must establish administrative mechanisms for persons to correct erroneous information about themselves; (4) agencies must annually report to OMB regarding the number, nature and handling of complaints.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G71
Acronym(s): DQA
Associated term(s): Information Quality

Data Recipient
A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP14

Data Retention Directive
This directive is designed to align the rules on data retention across the EU member states. It applies to traffic and location data but not to the actual content of communications of both individuals and organizations.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E43
Associated term(s): Directive 2006/24/EC

Data Subject
The individual about whom information is being processed, such as the patient at a medical facility, the employee of a company or the customer of a retail store.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F8; E63

GLOSSARY OF PRIVACY TERMS

De Novo
A Latin expression meaning “from the beginning,” “anew” or “beginning again.” In a legal context, a de novo hearing is one in which a higher authority can make a new decision, entirely ignoring the findings and conclusions of a lower authority.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C54-56

Deceptive Trade Practices
In the context of U.S. federal law, a term associated with corporate entities who mislead or misrepresent products or services to consumers and customers. These practices are regulated in the U.S. by the Federal Trade Commission at the federal level and typically by an attorney general or office of consumer protection at the state level. Law typically provides for both enforcement by the government to stop the practice and individual actions for damages brought by consumers who are hurt by the practices.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP70; US16
Associated term(s): Unfair Trade Practices
Associated law(s): U.S. Federal Trade Commission Act

Defamation
Common law tort which focuses on a false or defamatory statement, defined as a communication tending “so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.”

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US155
Associated term(s): Common Law

Deidentification
An action that one takes to remove identifying characteristics from data. De-identified data is information that does not actually identify an individual.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F5-7; IP37; US49
Associated term(s): Anonymization, Anonymized Data, Deidentified Data, Pseudonymization, Pseudonymized Data,
GLOSSARY OF PRIVACY TERMS

Derogation
The action by which an EU member state may deviate from certain directives, instead relying upon the domestic laws of member states.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E187

Digital Fingerprinting
The use of log files to identify a website visitor. It is often used for security and system maintenance purposes. Log files generally include: the IP address of the visitor; a time stamp; the URL of the requested page or file; a referrer URL, and the visitor’s web browser, operating system and font preferences. In some cases, combining this information can be used to “fingerprint” a device. This more detailed information varies enough among computing devices that two devices are unlikely to be the same. It is used as a security technique by financial institutions and others initiating additional security assurances before allowing users to log on from a new device. Some privacy enforcement agencies; however, have questioned what would constitute sufficient notice and consent for digital fingerprinting techniques to be used for targeted advertising.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US138

Digital Signature
A means for ensuring the authenticity of an electronic document, such as an e-mail, text file, spreadsheet or image file. If anything is changed in the electronic document after the digital signature is attached, the signature is rendered invalid.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US97; IP183

Direct Marketing
When the seller directly contacts an individual, in contrast to marketing through mass media such as television or radio.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F74-75; C36; E176

Acronym(s):


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

**Do Not Track**
A proposed regulatory policy, similar to the existing Do Not Call Registry in the United States, which would allow consumers to opt out of web-usage tracking.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F75, 134; US22, 24

Acronym(s): DNT

**Durant v. Financial Services Authority**
A court case in which the Court of Appeal of the United Kingdom narrowed the definition of personal data. It established a two-stage test; the information must be biographical in a significant sense and the individual must be the focus of the information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E54-55

---


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

Electronic Discovery
Prior to trial, information is typically exchanged between parties and their attorneys. E-discovery requires civil litigants to turn over large volumes of a company’s electronic records in litigation.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US133, 135-138
Associated term(s): Electronically, stored information (ESI), Sedona Conference
Associated law(s): Federal Rules of Civil Procedure

E-Government Act
A U.S. federal law that, among other things, requires federal agencies to conduct Privacy Impact Assessments on new or substantially revised information technology.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G67-68
Associated law(s): FISMA

Electronic Communications Data
Consists of three main categories of personal data: the content of a communication, traffic data and location data.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E229

Electronic Communications Network
Transmission systems, and, where applicable, switching or routing equipment and other resources that permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks; fixed and mobile terrestrial networks; electricity cable systems, to the extent that they are used for the purpose of transmitting signals; networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): Acronym(s): ECN
GLOSSARY OF PRIVACY TERMS

Electronic Communications Privacy Act of 1986
The collective name of the Electronic Communications Privacy and Stored Wire Electronic Communications Acts, which updated the Federal Wiretap Act of 1968. ECPA, as amended, protects wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The act applies to e-mail, telephone conversations and data stored electronically. The USA PATRIOT Act and subsequent federal enactments have clarified and updated ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US142,143; G32-36

Acronym(s): ECPA
Associated law(s): Stored Communications Act, Stored Wire Electronic Communications Act, USA Patriot Act

Electronic Communications Service
Any service which provides to users thereof the ability to send or receive wire or electronic communications.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Acronym(s): ECS

Electronic Health Record
A computer record of an individual's medical file that may be shared across multiple healthcare settings. In some cases this sharing can occur by way of network-connected enterprise-wide information systems and other information networks or exchanges. EHRs may include a range of data including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats such as age and weight and billing information. Their accessibility and standardization can facilitate large-scale data collection for researchers.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US52; C104

Acronym(s): EHR
Associated law(s): HIPAA, HITECH

Electronic Surveillance
Monitoring through electronic means; i.e., video surveillance, intercepting communications, stored

GLOSSARY OF PRIVACY TERMS

communications or location based services.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP145; US147, 157, 168
Associated law(s): Electronic Communications Privacy Act, Stored Communications Act, Wiretap Act

Employee Information
Personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating; (1) an employment relationship, or (2) a volunteer work relationship between the organization and the individual but does not include personal information about the individual that is unrelated to that relationship.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F39, 71-73; IP152, 251; US158-175; C17

Employee Personal Data
A high level of protection is required for employee personal data in the EU. The notice and choice principles of the EU Directive should be honored for all employee data, meaning that an employee should be given notice of the company's intent to share the information and give the employee the choice not to share this information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP251-252; E211-214

Employment at Will
An employment contract can be terminated by either the employer or the employee at any time for any reason.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US154

Encryption Key
A cryptographic algorithm applied to unencrypted text to disguise its value or to decrypt encrypted text.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
GLOSSARY OF PRIVACY TERMS

Encryption
The process of obscuring information, often through the use of a cryptographic scheme in order to make the information unreadable without special knowledge; i.e., the use of code keys.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F34, 88-89, 96-97, 124-125; IP164-165; US35

Equal Employment Opportunity Commission, The
An independent U.S. federal agency that enforces laws against workplace discrimination. The EEOC investigates discrimination complaints based on an individual's race, color, national origin, religion, sex, age, perceived intelligence, disability and retaliation for reporting and/or opposing a discriminatory practice. It is empowered to file discrimination suits against employers on behalf of alleged victims and to adjudicate claims of discrimination brought against federal agencies.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP119; US157

Acronym(s): EEOC

Established Business Relationship
An exemption to the Do Not Call (DNC) registry, a marketer may call an individual on the DNC registry if a prior or existing relationship formed by a voluntary two-way communication between a person or entity and a residential subscriber with or without an exchange of consideration, on the basis of an inquiry, application, purchase or transaction by the residential subscriber regarding products or services offered by such person or entity, which relationship has not been previously terminated by either party.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP53-54; US87, 95-96

Associated term(s): Established customer relationship

Established Service Provider
Under the E-Commerce Directive, an established service provider is a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E169
EU Data Protection Directive – see Data Protection Directive

EU Data Retention Directive – see Data Retention Directive

EU e-Privacy Directive – see e-Privacy Directive

EU Privacy and Electronic Communications Directive – see Privacy and Electronic Communications Directive

European Commission
The executive body of the European Union. Its main function is to implement the EU’s decisions and policies, along with other functions. It is also responsible for making adequacy determinations with regard to data transfers to third-party countries.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E274, 296

European Convention for the Protection of Human Rights and Fundamental Freedoms
A European convention that sought to secure the recognition and observance of the rights enunciated by the United Nations. The Convention provides that “(e)veryone has the right to respect for his private and family life, his home and his correspondence.” Article 8 of the Convention limits a public authority’s interference with an individual’s right to privacy, but acknowledges an exception for actions in accordance with the law and necessary to preserve a democratic society.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F3; IP3; C5; E29

European Convention on Human Rights
An international treaty among European states to protect human rights and fundamental freedoms. It applies only to member states.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP26; E5-6, 15

European Council
GLOSSARY OF PRIVACY TERMS

A forum where heads of state meet four times a year to define priorities and set political direction for the EU.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E24

European Court of Human Rights
An international court that oversees the European Convention on Human Rights and Fundamental Freedoms of 1950. The court is based in Strasbourg, France, and was set up in 1959.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

European Data Protection Supervisor
The EDPS is the data protection regulator for the EU as an entity. Established by EU regulation, the EDPS ensures that the institutions of the EU; i.e., the commission, council, Parliament, etc., respect the fundamental rights and freedoms of individuals, particularly their rights to privacy. Specifically, the job of the EDPS is to “monitor the application of the provisions of this Regulation to all processing operations carried out by a Community institution or body.”

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E200-204

Acronym(s): EDPS
Associated law(s): Regulation (EC) No 45/2001

European Economic Area
An economic region that includes the European Union (EU) and Iceland, Norway and Liechtenstein—which are not official members of the EU but are closely linked by economic relationship. Non-EU countries in the EEA are required to adopt EU legislation regarding the single market.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F46

Acronym(s): EEA

European Economic Community
Created by the Treaty of Rome, the EEC was a predecessor to the European Union that promoted a single economic market across Europe.


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Associated term(s): The Common Market

European Parliament
The only EU institution whose members are directly elected by member states, Parliament has four responsibilities—legislative development, supervisory oversight of other institutions, democratic representation and budget development.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E21
Acronym(s): MEP

European Union
The European Union replaced the EEC, created by the Treaty of Rome, the EEC promoted a single economic market across Europe. The EU is comprised of 27 member states including Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. Candidates include Croatia, the Former Yugoslav Republic of Macedonia, Iceland, Montenegro, Serbia and Turkey.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Acronym(s): EU

EU-U.S. Safe Harbor Agreement
An agreement between the EU and U.S. under which data may be exported to the U.S. in compliance with the EU Directive on Data Protection. Within a safe harbor agreement a data processor must abide by seven principles that and self-certify the compliance with to the Department of Commerce. These principles are notice, choice, consent to onward transfer, security, integrity, access, and enforcement. Certifying oneself as abiding by the Safe Harbor Framework without full compliance may be considered a deceptive trade practice under section 5 of the FTC Act.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F39-41; IP91, 250; US19; C114; E295
Associated term(s): Safe Harbor

**Extensible Markup Language**
A markup language that facilitates the transport, creation, retrieval and storage of documents. Similar to HTML, XML uses tags to describe the contents of a web page or file. XML describes content of a web page in terms of the data that is being produced, potentially creating automatic processing of data in ways that may require attention for privacy issues, unlike HTML, which describes the content of a web page in terms of how it should be displayed.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F116; IP208
Acronym(s): XML

**Extranet**
A network system formed through the connection of two or more corporate intranets. These external networks create inherent security risks, while often also meeting important organizational goals. An extranet opens a backdoor into the internal network and provides a third party with a level of trust. While these risks cannot be eliminated, they can be assessed, managed and mitigated. The foundation of this management is a thorough and detailed e-business contract that specifies who may access data, what data will be accessed and what security controls the partner has in place. It should also detail how shared devices will be managed, procedures for cooperating with technical staff in the event of problems and escalation procedures for resolving difficult technical problems.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F86-87; IP167-168
Factortame
A 1989 case brought before the European Court of Justice which established the precedence of EU law over national laws of member states in areas where the EU has competence.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E68

Fair Credit Reporting Act, The
One of the oldest U.S. federal privacy laws still in force today. It was enacted in 1970 to mandate accurate and relevant data collection, give consumers the ability access and correct their information, and limit the use of consumer reports to permissible purposes, such as employment and extension of credit or insurance.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F4, 42; IP27-28; US57-64; C123-124
Acronym(s): FCRA

Fair Information Practices
(1) The Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. (2) The Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. (3) The Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. (4) The Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 8 (below) except a) with the consent of the data subject, or b) by the authority of law. (5) The Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. (6) The Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller. (7) The Individual Participation Principle. An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him; c) to be given...
reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such
denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data
erased, rectified, completed or amended; (8) The Accountability Principle. A data controller should be
accountable for complying with measures which give effect to the principles stated above.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F15-22; IP10-13; C18-20;
E8-9
Acronym(s): FIPs

---

**Fairness**

One of two requirements established by the EU Data Protection Directive for the processing of personal
data. In order to be considered fair, the data controller must provide specific information to the data
subject prior to processing.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  E82-83
Associated term(s): Data Controller, Lawfulness
Associated law(s): Data Protection Directive

---

**FCRA** — see Fair Credit Reporting Act

**Federal Advisory Committee Act, The**

A federal law governing the behavior of federal advisory committees, restricting the formation of such
committees to those deemed essential, limiting their powers and their length of operation, requiring
open meetings and open records and mandating a publicly-accessible government-wide database.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G77
Acronym(s): FACA

---


A U.S. federal law enacted as part of the E-Government Act of 2002. The act requires each federal
agency to develop, document and implement an agency-wide program to provide information security
for the data and data systems that support the operations and assets of the agency, including those
provided or managed by another agency, contractor or other source. FISMA requires agency program
officials, chief information officers and inspectors general to conduct annual reviews of the agency’s
information security program and report the results to Office of Management and Budget. OMB uses this
data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency
compliance with the act. In FY 2008, federal agencies spent $6.2 billion securing the government’s total
information technology investment of approximately $68 billion or about 9.2 percent of the total

Textbook key: F=Foundations of Information Privacy and Data Protection, IP=Information Privacy, US=U.S. Private-sector Privacy,
C=Canadian Privacy, E=European Privacy, G=U.S. Government Privacy, IT=Privacy in Information Technology; M=Managing Privacy

IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

Federal Information Security Incident Center
FISMA codified a federal information security center, which is implemented in the U.S. Computer Emergency Readiness Team (US-CERT). U.S.-CERT is called upon to provide timely technical assistance regarding security incidents; compile and analyze security incident information; inform federal agency information system operators about current and potential threats, and consult with NIST and others regarding information security incidents.

Federal Trade Commission
The United States' primary consumer protection agency, the FTC collects complaints about companies, business practices and identity theft under the FTC Act and other laws that they enforce or administer. Importantly, the FTC brings actions under Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices.

Final Health Breach Notification Rule
A rule, promulgated under HITECH, requiring vendors of personal health records and related entities to notify consumers when the security of their individually identifiable health information has been breached.
GLOSSARY OF PRIVACY TERMS

**FISMA** – *See Federal Information Security Management Act*

**Flash**
Software that is used to add animation and other visual effects to web-based content.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F119; IP202

**Foreign Intelligence Surveillance Act of 1978, The**
A U.S. federal law regulating the way that U.S. intelligence agencies conduct foreign intelligence surveillance activities, including wiretaps and the interception of communications. The act sets forth a judicial approval process required when the government targets U.S. persons located within the United States. FISA allows warrantless surveillance to be conducted without a court order for up to one year, provided the surveillance is for foreign intelligence information, is targeting foreign powers and will not capture the contents of any communication to which a U.S. person is a party. Generally speaking, FISA does not apply to activities directed at persons overseas.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G29-31

Acronym(s):  FISA

**Four Classes of Privacy**
Four main areas of privacy are of particular interest with regard to data protection and privacy laws and practices: information privacy, bodily privacy, territorial privacy, and communications privacy.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F2; IP2

**Freedom of Information Act, The**
A U.S. federal law that ensures citizen access to federal government agency records. FOIA only applies to federal executive branch documents. It does not apply to legislative or judicial records. FOIA requests will be fulfilled unless they are subject to nine specific exemptions. Most states have some state level equivalent of FOIA. The federal and most state FOIA statutes include a specific exemption for personal information so that sensitive data (such as Social Security numbers) are not disclosed.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F44; IP80; US133-135; G37-47

Acronym(s):  FOIA
GLOSSARY OF PRIVACY TERMS

Freely-Given Consent
Consent that is given when the data subject has a genuine choice and there is no risk of coercion, deception, or intimidation if the data subject does not consent.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E93
Glossary of Privacy Terms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Gaskin v. United Kingdom
A court case in which it was decided the restriction of an applicant’s access to their file was contrary to article 8 of the European Convention on Human Rights.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E31

Generally Accepted Privacy Principles
A framework promulgated by the American Institute of Certified Public Accountants (AICPA) in conjunction with the Canadian Institute of Chartered Accountants (CICA). The ten principles are management, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security for privacy, quality, monitoring and enforcement.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C61-62

Acronym(s): GAPP

GET method
The GET and POST HTML method attributes specify how form data is sent to a web page. The GET method appends the form data to the URL in name/value pairs allowing passwords and other sensitive information collected in a form to be visible in the browser’s address bar, and is thus less secure than the POST method.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  
Associated term(s): POST Method

Global Privacy Enforcement Network
GPEN aims to promote cross-border information sharing as well as investigation and enforcement cooperation among privacy authorities around the world. Another cross-border enforcement cooperation effort is the Asia-Pacific Economic Cooperation.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US25

Acronym(s): GPEN


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
Government Forum of Incident Response and Security Teams
A group of more than 50 incident response teams from federal government agencies responsible for securing government information technology systems. This group is among those with whom US-CERT works.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): Acronym(s): GFIRST
Associated term(s): Federal Information Security Incident Center
Associated law(s): FISMA

Government in the Sunshine Act
The Government in the Sunshine Act, 5 U.S.C. § 552b, generally requires multi-member federal agencies; i.e., the FCC and SEC, to hold their meetings in public and to give advance public notice of their meetings. The goal of the Sunshine Act is to promote public access to information about the decision-making processes of the federal government and to improve those processes by exposing them to public view.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): Acronym(s): GSA
Associated term(s): 5 U.S.C. § 552b

Gramm-Leach-Bliley Act
The commonly used name for The Financial Services Modernization Act of 1999. The act re-organized financial services regulation in the United States and applies broadly to any company that is “significantly engaged” in financial activities in the U.S. In its privacy provisions, GLBA addresses the handling of non-public personal information, defined broadly to include a consumer's name and address, and consumers' interactions with banks, insurers and other financial institutions. GLBA requires financial institutions to securely store personal financial information; give notice of their policies regarding the sharing of personal financial information, and give consumers the ability to opt out of some sharing of personal financial information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): Acronym(s): GLBA
Haralambie v. Romania
A court case claiming that the Romanian government violated Article 8 of the European Convention on Human Rights by placing of obstacles in the way of an applicant when he sought access to the file on him drawn up by the Communist government’s secret service.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E31

Health Information Technology for Economic and Clinical Health Act, The
The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to healthcare information technology in general; i.e., the creation of a national healthcare infrastructure, and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F32; IP35-40; US51-52; C124-125; G15-18

Acronym(s): HITECH
Related term(s): EHR
Associated law(s): HIPAA

Health Insurance Portability and Accountability Act, The
A U.S. law passed to create national standards for electronic healthcare transactions, among other purposes. HIPAA required the U.S. Department of Health and Human Services to promulgate regulations to protect the privacy and security of personal health information. The basic rule is that patients have to opt-in before their information can be shared with other organizations—although there are important exceptions such as for treatment, payment and healthcare operations.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F42; IP35-40; US46-51; C124-125; G15-18

Acronym(s): HIPAA

House of Commons
One of two chambers of the Canadian Parliament, along with the Senate. Members of the House of Commons are elected at least every five years.
Human Resources Data Management
Management encompasses many different considerations including legal compliance with the many laws that regulate employee data and the employment relationship, protection of human resources data from unauthorized use and authorized misuse, proper documentation to manage any potential claims against the company or that the company may have against its employees, and compliance with other corporate policies including substantive training, workplace liability management, and document retention.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
C7

Hyperlink
Linked graphic or text that is used to connect an end user to other websites, parts of websites or web-enabled services. The URL of a web location is embedded in the HTML code, so that when certain words or images are selected through the web browser, the end user is transported to the destination website or page.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
F117; IP199

Hypertext Markup Language (HTML)
A content authoring language used to create web pages. Web browsers use HTML to interpret and render visible and audible content from the web pages. Document “tags” can be used to format and lay out web page content and to “hyperlink”—connect dynamically—to other web content. Forms, links, pictures and text may all be added with minimal commands. Headings are also embedded into the text and are used by web servers to process commands and return data with each request.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
F116; IP199

Acronym(s):
HTML

Associated term(s):
HTTP, HTTPS
GLOSSARY OF PRIVACY TERMS

formatted and transmitted over a TCP/IP network for websites. Further, it defines what actions Web servers and web browsers take in response to various commands.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F115
Acronym(s): HTTP
Associated term(s): HTML, HTTPS

Hypertext Transfer Protocol Secure
A secure network communication method, technically not a protocol in itself, HTTPS is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F118
Acronym(s): HTTPS
Associated term(s): HTTP, SSL/TLS

Identifying Purposes
Integral to privacy protection is the obligation on organizations to identify and document the purposes for the collection of any personal information at or before the time of collection.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C19

Individual Access
One of 10 privacy principles of PIPEDA. Organizations must be able to respond to requests from individuals for access to their personal information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C19-20

Associated law(s): PIPEDA

Individual Participation
A fair information practices principle, it is the principle that an individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have data relating to him communicated to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F18; IP11; E20

Associated term(s): FIPPs

Information Banks
Repositories of personal information that are kept by the Canadian government to comply with the Privacy Act.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C72

Associated law(s): The Canadian Privacy Act

GLOSSARY OF PRIVACY TERMS

**Information Lifecycle**
(1) Collection; (2) Use and Retention; (3) Disclosure.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F13, 16

**Information Privacy**
One of the four classes of privacy, along with territorial privacy, bodily privacy, and communications privacy. The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F2-4, 77-78; IP2

**Information Security**
The protection of information for the purposes of preventing loss, unauthorized access and/or misuse. It is also the process of assessing threats and risks to information and the procedures and controls to preserve confidentiality, integrity and availability of information.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F77-112
Acronym(s): IS

**International Data Transfers**
The transmission of personal information from one jurisdiction to another. Many jurisdictions, most notably the European Union, place significant restrictions on such transfers. The EU requires that the receiving jurisdiction be judged to have “adequate” data protection practices.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F19, 36-37; E175-178

**Internet Protocol Address**
A unique string of numbers that identifies a computer on the Internet or other 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. An address may be "dynamic," meaning that it is assigned temporarily whenever a device


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
logs on to a network or an Internet service provider and consequently may be different each time a device connects. Alternatively, an address may be "static," meaning that it is assigned to a particular device and does not change, but remains assigned to one computer or device.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F6-7, 118; IP201; E278-279

Acronym(s): IP Address

Internet Service Provider
A company that provides Internet access to homes and businesses through modem dial-up, DSL, cable modem broadband, dedicated T1/T3 lines or wireless connections.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F7, 118

Acronym(s): ISP

Intrusion Detection System
A system that inspects network activity and identifies suspicious patterns that may someone is attempting to penetrate or compromise a system or network. An IDS: may be network-based or host-based; signature-base or anomaly-based, and requires human intervention in order to respond to the attack.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F99-101; IP164, 188

Acronym(s): IDS

Associated term(s): Intrusion Prevention System (IPS)

Intrusion Prevention System
A form of access control. An IPS is much like an application firewall. Its intent is not only to detect a network attack but to prevent it. It neither requires nor involves human intervention in order to respond to a system attack.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F99-101; IP188

Acronym(s): IPS

Associated term(s): Intrusion Detection System (IDS)

ISO 27002
The ISO (International Organization for Standardization) 27002 standard is a code of practice for

GLOSSARY OF PRIVACY TERMS

information security with hundreds of potential controls and control mechanisms. The standard is intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F81-82


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
JJavascript
A computer scripting language used to produce interactive and dynamic web content.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F118-119; IP200

Jurisdiction
The authority of a court to hear a particular case. Courts must have jurisdiction over both the parties to
the dispute (personal jurisdiction) and the type of dispute (subject matter jurisdiction). The term is also
used to denote the geographical area or subject-matter to which such authority applies.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F6-7; IP20; US5; C8

Just-in-Time Notification
Disclosure of specific information practices posted, usually accompanied by a consent request, at the point
of information collection

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F122; IP20; C8

Acronym(s):
JIT Notice
### Law Enforcement Authority
A body sanctioned by local, regional or national governments to enforce laws and apprehend those who break them. In Europe, public law enforcement authorities are governed by strict rules of criminal procedure designed to protect the fundamental human right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR).

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E227
Associated term(s): **Public Law Enforcement Authorities**
Acronym(s): LEA

### Lawfulness
According to the EU Data Protection Directive, processing of personal data must meet two specific requirements; fairness and lawfulness. Lawfulness suggests a community-wide set of norms enforceable by the intervention of the state. In order to be lawful, processing must meet all legal requirements.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E83-85
Associated term(s): **Fairness**
Associated law(s): **Data Protection Directive**

### Layered Security Policy
A layered approach defines three levels of security policies. The top layer is a high-level document containing the controller’s policy statement. The next layer is a more detailed document that sets out the controls that will be implemented to achieve the policy statements. The third layer is the most detailed and contains the operating procedures, which explain how the policy statements will be achieved in practice.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E152-153

### Layered Notice
A privacy notice designed to respond to problems with a excessively long notices. A short notice—the top layer—provides a user with the key elements of the privacy notice. The full notice—the bottom layer—covers all the intricacies in full. In Europe, the [Article 29 Working party](https://www.article29.eu/) recommends three layers: a short notice, a condensed notice and a full notice.
GLOSSARY OF PRIVACY TERMS

Least Privilege
A security control where access is granted at the lowest possible level required to perform the function.

Legitimate Interests of Controller
One of several legitimate processing criteria required by the EU Data Protection Directive. This rather broad criteria states “Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject, which require protection under Article 1(1).”

Legitimate Processing Criteria
To process data in compliance with EU data protection law, a controller must be able to base the processing activity on at least one legitimate criteria derived from the Data Protection Directive. These criteria are consent, necessity, contract requirement, legal obligation, protection of data subject, public interest and legitimate interests of the controller.

Limiting Use
The concept that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law.
GLOSSARY OF PRIVACY TERMS

Lindqvist Judgement
A case in which the European Court of Justice ruled that a woman who identified and included information about fellow church volunteers on her website was in breach of the Data Protection Directive 95/46/EC. The ECJ held that the creation of a personal website was not a personal activity allowing the woman to be exempted from the data protection rules.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E32-33, 74
Associated law(s): Directive 95/46/EC

Local Area Network
Networks that exist within an operational facility. They are considered within local operational control and are relatively easy to manage.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F85-86; IP167
Acronym(s): LAN
Associated term(s): WAN

Location-Based Service
Services that utilize information about location to deliver, in various contexts, a wide array of applications and services, including social networking, gaming and entertainment. Such services typically rely upon GPS, RFID or similar technologies in which geolocation is used to identify the real-world geographic location of an object, such as a cell phone or an Internet-connected computer terminal.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F141; US170; E242-245
Acronym(s): LBS
Associated term(s): Geolocation; GPS; Global Positioning System; RFID

Logs
A record of both normal and suspect events by a computer system (typically an operating system). The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The program developer decides which events to record. The system log contains events logged by the operating system components; for example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined for the operating system. The security log can record


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

security events, such as valid and invalid log-in attempts as well as events related to resource use, such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled log-in auditing, attempts to log in to the system are recorded in the security log.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F80, 101, 106
Machine-readable Formats
"[W]ritten in a standard computer language (not English text) that can be read automatically by a web browser." (Source: OMG PIA Guidance)

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G57, G67-68

Madrid Resolution
A resolution that was adopted by the International Conference of Data Protection and Privacy Commissioners, consisting of 80 data protection authorities from 42 countries around the world, including members of the Article 29 Working Party. Principles include: lawfulness and fairness; purpose specification; proportionality; data quality; openness; accountability.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F22

Matching Program (from The Privacy Act of 1974)
Under the Privacy Act, it is "[a]ny computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs, or two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records." Excluded from the term are (1) matches performed aggregate statistical data; (2) research or statistical projects that will not be used for decision marked regarding specific individuals; (3) matches performed by criminal law enforcement subsequent to the initiation of a specific person or group of people; (4) matches of tax information pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act; (5) matches using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or conducted by an agency using only records from systems of records maintained by that agency if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;
(6) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; (7) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or (8) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1).”

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G48-49
Associated term(s): The Privacy Act of 1974

Medical Information
Information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics or other medical or medically related facilities.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F67-68, US45-47, 63; G15-18
Associated term(s): HIPAA

Members of the European Parliament
MEPs have the right to propose written and oral questions to the European Council and the European Commission providing another layer of oversight in the legislative process.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  E22-23
Acronym(s): MEPs

Memorandum of Understanding/Agreement
“A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide [NIST SP 800-47], an MOU/A defines the responsibilities of two or more organizations in establishing, operating and securing a system interconnection.”

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G143
Acronym(s): MOU
Associated term(s): NIST SP 800-47

Minimum Necessary Requirement
GLOSSARY OF PRIVACY TERMS

Under HIPAA, the standard that the level of information that may be disclosed by healthcare providers to third parties is the minimum amount necessary to accomplish the intended purpose.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F22; IP37; US47-48
Associated term(s): Minimum Necessary Standard
Associated law(s): HIPAA

Mission Critical System
Defined in 44 U.S.C. §3532 as "(a)ny telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that: (A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an executive order or an Act of Congress to be classified in the interest of national defense or foreign policy, or(C) processes any information, the loss, misuse, disclosure or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency."

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

Model Code for the Protection of Personal Information
A set of privacy principles developed by the Canadian Standards Association, that parallel the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and espouse 10 principles: Accountability, Identifying Purpose, Consent, Limiting Collection, Limiting Use, Disclosure, & Retention, Accuracy, Safeguards, Openness, Individual Access and Challenging Compliance

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C19, 146

Monetary Instrument Log
Under the Bank Secrecy Act, the log of transactions a financial institution must retain a record for cash purchases of monetary instruments (e.g., money orders, cashier’s checks, travelers checks) ranging from $3,000 to $10,000.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G27
Acronym(s): MIL
Associated law(s): Bank Secrecy Act


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
**Motor Vehicle Record**

"(A)ny record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration or identification card issued by a department of motor vehicles."

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

F, US, C, E, G, IT, M

**Multi-Factor Authentication**

The authentication of a user by multiple means. This is typically accomplished by a requirement for both a password and at least one other form of authentication such as a pass card, biometric scan or an "out of band" means such as a phone call.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F94-95; IP183, G94

Associated term(s): Two-Factor Authentication; Two-Step Authentication

**Multi-State Information Sharing & Analysis Center**

A voluntary and collaborative organization with participation from all 50 states and the District of Columbia. The MS-ISAC provides a central resource for gathering from the states information on cyber threats to critical infrastructure and sharing that information among state and local governments.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G96

Acronym(s): MS-ISAC

Associated term(s): US-CERT

F, US, C, E, G, IT, M
National Labor Relations Board, The
A U.S. federal agency that administers the National Labor Relations Act. The board conducts elections to determine if employees want union representation and investigates and remedies unfair labor practices by employers and unions.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP120; US157
Acronym(s): NLRB
Associated law(s): NLRA

National Security Letter
A category of subpoena. The USA PATRIOT Act expanded the use of NSLs. Separate and sometimes differing statutory provisions now govern access, without a court order, to communication providers, financial institutions, consumer credit agencies and travel agencies.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US148
Acronym(s): NSL
Associated law(s): USA-PATRIOT Act

Negligence
An organization will be liable for damages if it breaches a legal duty to protect personal information and an individual is harmed by that breach.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F25; US5
Associated term(s): Private Right of Action

Network-Layer Attacks
Attacks that exploit the basic network protocol in order to gain any available advantage. These attacks generally involve “spoofing” a network address so that a computer sends data to an intruder rather than their proper recipient or destination. Other attacks can involve service disruptions through a denial of service (DOS) attack—a brute force method that overloads the capacity of a website’s domain to respond to incoming requests such that it renders the server inoperable.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F102; IP191
**Non-Public Personal Information**

Is defined by GLBA as personally identifiable financial information (i) provided by a consumer to a financial institution, (ii) resulting from a transaction or service performed for the consumer, or (iii) otherwise obtained by the financial institution. Excluded from the definition are (i) publicly available information and (ii) any consumer list that is derived without using personally identifiable financial information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F43; IP41; US67-68

Acronym(s): NPI

Associated law(s): GLBA

**Non-Repudiation**

The ability to ensure that neither the originator nor the receiver in a transaction can dispute the validity of the transaction or access request. An independent verification takes place which allows the sender’s identity to be verified, typically by a third party, and also allows the sender to know that the intended recipient of the message actually received it. Non-repudiation of origin proves that data has been sent and non-repudiation of delivery proves that the data has been received.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F94; IP177

**Notification (EU)**

(Three-fold purpose) The process by which information about data controllers and their personal data processing operations comes to be included in a publicly-accessible register maintained by the relevant national DPA.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E163-164
GLOSSARY OF PRIVACY TERMS

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

OECD Guidelines

(1) The Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. (2) The Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. (3) The Purpose Specification Principle. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. (4) The Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 8 (below) except a) with the consent of the data subject; or b) by the authority of law. (5) The Security Safeguards Principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. (6) The Openness Principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. (7) The Individual Participation Principle. An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial, and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. (8) The Accountability Principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F17-18; US13; E7-9

Associated term(s): OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (1980), The

Omnibus Laws

Laws in which the government has defined requirements throughout the economy including public-sector, private-sector and health-sector.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US16


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
**Online Behavioral Advertising**
Websites or online advertising services that engage in the tracking or analysis of search terms, browser or user profiles, preferences, demographics, online activity, offline activity, location data, etc., and offer advertising based on that tracking.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F134; IP210-211; US22, 24; C45-47; E261-264

**Online Privacy Alliance**
A coalition composed of numerous online companies and trade associations specifically established to encourage the self-regulation of online privacy. The OPA introduced the Online Privacy Guidelines.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C5-6

Acronym(s): OPA

Associated term(s): Self-regulation

**Openness**
A fair information practices principle, it is the principle that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F18, 22; IP12; C42-43; E8

**Opinion 1/2003**
An Article 29 Working Party opinion on the storage of traffic data for billing purposes that recommends that telecommunications service providers ordinarily store personal traffic data for a maximum period of three to six months, except for disputed cases, where data may be processed for longer.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E91

**Opinion 1/2008**
An Article 29 Working Party opinion that advises search engine providers to keep data for a maximum period of six months and to provide justifications for such retention periods. Therefore, when search

engine providers intend to keep data for longer than six months, the Article 29 Working Party recommends they demonstrate comprehensively that it is strictly necessary for the service.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E91

Opinion 1/2010
A 2010 Article 29 Working Party opinion on the concepts of “controller” and “processor” that provides assistance to organisations operating in the European Union when engaging service providers and when acting as a service provider. The distinction between controller and processor is crucial as it determines who is responsible for compliance with data protection law and dealing with data subjects’ rights, the applicable law and the enforcement actions of data protection authorities.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

Opinion 2/2010
An Article 29 Working Party on online behavioural advertising adopted on 22 June 2010, the Article 29 Working Party states that Article 6(1)(e) requires data to be deleted when it is no longer necessary for the purpose for which the data was collected. Compliance with this principle requires limiting the storage of information. Accordingly, it states that companies must specify and respect express timeframes under which data will be retained. Pursuant to this, information about users’ behaviour has to be eliminated if it is no longer needed for the development of a profile.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E91

An Article 29 Working Group opinion the concept of personal data, the European Union aimed for a ‘wide notion’ of the concept of personal data so as to include all information concerning an identifiable individual. On that basis, the concept embraces considerable amounts of information, even where the link between such information and an identifiable individual is tenuous.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

Opt-In
One of two central concepts of choice. It means an individual makes an active affirmative indication of

IAPP Privacy Glossary, © 2012
Version 2.0.0.2
choice; i.e., checking a box signaling a desire to share his or her information with third parties.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F16; IP8-9; US38-40; C116-117; E136; G151

Associated term(s): Choice; Consent; Opt-Out

**Opt-Out**

One of two central concepts of choice. It means that an individual’s lack of action implies that a choice has been made; i.e., unless an individual checks or unchecks a box, his or her information will be shared with third parties.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F16; IP8-9; US38-40; C116-117; E136; G151

Associated term(s): Choice; Consent; Opt-In

**Organization for Economic Cooperation and Development**

An international organization that promotes policies designed to achieve the highest sustainable economic growth, employment and a rising standard of living in both member and non-member countries, while contributing to the world economy.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F17-18; IP11-12, 230; US13, 24; C18; E7; G6-8

Acronym(s): OECD

**Outsourcing**

Contracting business processes, such as the processing of personal information, to a third party.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C88-89; E287-292


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
Passive Data Collection
Data collection in which information is gathered automatically—often without the end user's knowledge—as the user navigates from page to page on a website. This is typically accomplished through the use of cookies, web beacons or other types of identification mechanisms.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F128; IP203-204
Associated term(s):  Observational Study;  Cookie;  Web Beacons;  Active Data Collection

PCI Data Security Standard
A self-regulatory system that provides an enforceable security standard for payment card data. The rules were drafted by the Payment Card Industry Security Standards Council, which built on previous rules written by the various credit card companies. Except for small companies, compliance with the standard requires hiring a third party to conduct security assessments and detect violations. Failure to comply can lead to exclusion from Visa, MasterCard or other major payment card systems, as well as penalties.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F33; US23, 117
Acronym(s):  PCI-DSS

Perimeter Controls
Technologies and processes that are designed to secure an entire network environment by preventing penetration from the outside.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F100; IP187-188
Associated term(s):  Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Internet Protocol Security (IPSEC), Secure Sockets Layer (SSL)

Personal Data
Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly—in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F4-7, 39
Associated term(s):  Personal Information; Personally Identifying Information; Personally Identifiable Information
GLOSSARY OF PRIVACY TERMS

Personal Information
May refer to either a generic term for information, or an EU term for such information. In the U.S., such information may be referred to as Personally Identifiable Information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F4-7, 39; IP7, 98
Acronym(s): PI
Associated term(s): Personal Data; Personally Identifying Information; Personally Identifiable Information

Personal Information Protection and Electronic Documents Act
A Canadian act with two goals: (1) to instill trust in electronic commerce and private sector transactions for citizens, and (2) to establish a level playing field where the same marketplace rules apply to all businesses.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F48-49; IP81-83; C23-31
Acronym(s): PIPEDA

Phishing
E-mails or other communications that are designed to trick a user into believing that he or she should provide a password, account number or other information. The user then typically provides that information to a website controlled by the attacker. “Spear phishing” is a phishing attack that is tailored to the individual user, such as when an e-mail appears to be from the user's boss, instructing the user to provide information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F119, 132; IP213-214
Associated term(s): Spear Phishing; Social Engineering

PIA Triggers
These events constitute triggers for an organization to conduct a privacy impact assessment: Conversion of records from paper-based to electronic form; Conversion of information from anonymous to identifiable form; System management changes involving significant new uses and/or application of new technologies; Significant merging, matching or other manipulation of multiple databases containing PII; Application of...
GLOSSARY OF PRIVACY TERMS

user-authenticating technology to a system accessed by members of the public; Incorporation into existing databases of PII obtained from commercial or public sources; Significant new inter-agency exchanges or uses of PII; Alteration of a business process resulting in significant new collection, use and/or disclosure of PII; Alteration of the character of PII due to the addition of qualitatively new types of PII.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G62
Associated law(s): FISMA

Policy Framework
The repository of all an organization’s rules for confidentiality and security. It is the natural reference point for anyone who wants to understand an organization’s position.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E151-153

Polygraph
A device used for the purpose of rendering a diagnostic opinion regarding an individual’s honesty.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Associated term(s): Lie Detector
Associated law(s): Employee Polygraph Protection Act of 1988 (EPPA)

POST Method
The GET and POST HTML method attributes specify how form data is sent to a web page. The POST method is more secure than GET as the GET method appends the form data to the URL allowing passwords and other sensitive information collected in a form to be visible in the browser’s address bar.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): Refs
Associated term(s): GET Method

Postal Marketing
Direct marketing to postal addresses. Data controllers must also ensure that they satisfy the general compliance requirements of the Data Processing Directive when processing individuals’ personal data to


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

send postal marketing, including the transparency requirement and the lawful processing requirement. Because postal marketing is not digital, it is not subject to the requirements of the e-Privacy Directive.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  E253
Associated term(s):  Direct Marketing
Associated law(s):  Data Processing Directive

Preemption
A superior government’s ability to have its law(s) supersede those of an inferior government. For example, the U.S. federal government has mandated that no state government can regulate consumer credit reporting.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  IP21; US6

Prior Authorisation
Some data processing operations may present specific risks to the rights and freedoms of data subjects and thus require ‘prior checking’ and approval from the national Data Protection Authority (DPA) before the data processing activity can commence. Such prior checking is carried out by the DPA following receipt of a notification from the data controller or data protection official.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  E167
Associated term(s):  Notification; Data Protection Authority

Privacy Act Exceptions
Among the exception to the Privacy Act of 1972 are: (1) Performance of regular duties of an agency employee; (2) FOIA disclosures; (3) Routine uses as specified in the applicable SORN; (4) Census Bureau census or survey functions; (5) Statistical research if not individually identifiable(6) Data held by the National Archives; (7) Law enforcement activity; (8) Compelling health or safety circumstances; (9) Congressional committee with appropriate jurisdiction; (10) GAO duties; (11) Court order, and (12) Consumer reporting agencies;

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  G52
Associated term(s):  Privacy Act of 1972, The
Associated law(s):  Privacy Act of 1972, The

GLOSSARY OF PRIVACY TERMS

Privacy Act of 1974, The
A U.S. law that regulates the federal government’s use of computerized databases of information about U.S. citizens and permanent legal residents. It also establishes fair information practices that each agency must follow when collecting, using or disclosing personal information, including rights of citizen action and redress for violations. It guarantees that U.S. citizens and lawful permanent residents have: (1) the right to see records about themselves that are maintained by the federal government (provided that information is not subject to one or more of the Privacy Act’s exemptions); (2) the right to amend inaccurate, irrelevant, untimely or incomplete records; and (3) the right to sue the government for failure to comply with its requirements. It also contains fair information practices that: (1) require that information about a person be collected from that person to the greatest extent practicable; (2) require agencies to ensure that their records are relevant, accurate, timely and complete; and (3) prohibit agencies from maintaining information describing how an individual exercises his or her First Amendment rights (unless the individual consents to it, it is permitted by statute or is within the scope of an authorized law enforcement investigation).

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F43-44, 70; IP79; US13; G48-57

Privacy Act, The (Canadian)
Enacted in 1983, the Act sets out rules for how institutions of the federal government must deal with personal information of individuals. It has been revised by many minor amendments, but remains substantially unaltered.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C67

Privacy Assessment
An assessment of an organization’s compliance with its privacy policies and procedures, applicable laws, regulations, service-level agreements, standards adopted by the entity and other contracts. The assessment or audit measures how closely the organization’s practices align with its legal obligations and stated practices and may rely on subjective information such as employee interviews/questionnaires and complaints received, or objective standards, such as information system logs or training and awareness attendance and test scores. Audits and assessments may be conducted internally by an audit function or by external third parties. It is also common in some jurisdictions for the privacy/data protection officer to conduct assessments. The results of the assessment or audit are documented for management sign-off, and analyzed to develop recommendations for improvement and a remediation plan. Resolution of the issues and vulnerabilities noted are then monitored to ensure appropriate corrective action is taken on a timely basis. While assessments and audits may be conducted on a regular or scheduled basis, they may also arise ad hoc as the result of a privacy or security event or due to a request from an enforcement authority.


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
Privacy Breach Response (Canadian)
The guidelines for privacy breach responses were drafted in 2007 and consist of four steps: (1) Containment of the breach and preliminary assessment; (2) evaluating the associated risks; (3) notifying affected parties; (4) taking adequate steps to prevent future breaches.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C60, 138
Associated term(s): Data Breach, Privacy Breach (Canadian)

Privacy Breach (Canadian)
A privacy breach occurs when there is unauthorized access, collection, use or disclosure of personal information. Such activity is “unauthorized” if it occurs in contravention of applicable privacy legislation, such as PIPEDA or similar provincial privacy legislation.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C137
Associated term(s): Data Breach, Privacy Breach Response (Canadian)

Privacy by Design
The concept that organizations need to build privacy directly into technology, systems and practices at the design phase, thereby ensuring the existence of privacy from the outset. Originating in the mid-1990s by the Information and Privacy Commissioner of Ontario, the principle has gained recognition around the globe, including from the U.S. Federal Trade Commission and the European Commission. Privacy by Design consists of seven foundational principles: (1) Proactive not Reactive; Preventative not Remedi. Privacy by Design anticipates and prevents privacy invasive events before they happen, rather than waiting for privacy risks to materialize; (2) Privacy as the Default Setting. No action is required by individuals to maintain their privacy; it is built into the system by default. This concept has been introduced in the European Commission’s draft regulation to reform data protection. (3) Privacy Embedded into Design. Privacy is an essential component of the core functionality being designed and delivered. The FTC has adopted this principle in its proposed consumer privacy framework, calling for companies to promote consumer privacy throughout the organization and at every stage of product development. (4) Full Functionality—Positive-Sum, not Zero-Sum: Privacy by Design seeks to accommodate all legitimate interests and objectives, rather than making unnecessary trade-offs. (5) End-to-End Security—Full Lifecycle Protection. Strong security measures are essential to privacy, from start to finish of the lifecycle.
GLOSSARY OF PRIVACY TERMS

of data. This is another principle the FTC has adopted in its proposed consumer privacy framework.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F14-15, 128; US21
Acronym(s): PbD

Privacy Commissioner of Canada
The individual who is mandated by PIPEDA to enforce the act. The commissioner has broad power to
examine documents, but some documents may be shielded by solicitor-client privilege. The commissioner
conducts investigations under a cloak of confidentiality, but public reports with non-binding
recommendations are ultimately issued. This individual is mandated by PIPEDA to enforce PIPEDA.
Aggrieved individuals also have a right to complain to the commissioner.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C30
Associated law(s): PIPEDA

Privacy Impact Assessment
"An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory
and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining
and disseminating information in identifiable form in an electronic information system, and (iii) to examine
and evaluate protections and alternative processes for handling information to mitigate potential privacy
risks." PIAs should disclose what PII is being collected, why it is being collected, what the intended uses of
the PII are, whom the PII will be shared with, what opportunities individuals will have to opt-out of PII
collection or use, how the PII will be secured, whether a system of records is being created under the
Privacy Act and an analysis of the information life cycle. Checklists or tools used to ensure that the system
used to collect personal information is evaluated for privacy risks, designed with lifecycle principles in
mind and made to ensure that effective and required privacy protection measures are used. A PIA should
be completed pre-implementation of the privacy project, product, or service and should be ongoing
through its deployment. The PIA should identify these attributes of the data collected: what information is
collected; why it is collected; the intended use of the information; with whom the information is shared,
and the consent and choice rights of the data subjects. The PIA should be used to assess new systems,
significant changes to existing systems, operational policies and procedures and intended use of the
information. PIAs should also be used before, during, and after mergers and acquisitions. An effective PIA
evaluates the sufficiency of privacy practices and policies with respect to existing legal, regulatory and
industry standards, and maintains consistency between policy and operational practices.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F14; G57-61, 130-137
Acronym(s): PIAs

Textbook key: F=Foundations of Information Privacy and Data Protection, IP=Information Privacy, US=U.S. Private-sector Privacy,
C=Canadian Privacy, E=European Privacy, G=U.S. Government Privacy, IT=Privacy in Information Technology; M=Managing Privacy

IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

Privacy Impact Assessments (Canadian)
The Canadian government requires all government institutions subject to the Privacy Act to conduct these assessments. The purpose behind a PIA is to evaluate whether program and service delivery initiatives that involve the collection, use or disclosure of personal information are in compliance with statutory obligations.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Acronym(s): PIAs

Privacy Notice
A statement made to a data subject that describes how the organization collects, uses, retains and discloses personal information. A privacy notice is sometimes referred to as a privacy statement, a fair processing statement or sometimes a privacy policy. Special privacy notices are also mandated by specific laws such a GLBA and COPPA in the United States.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F16; US16-18, 37

Privacy of the Person
Protects bodily integrity, and in particular the right not to have our bodies touched or explored to disclose objects or matters we wish to conceal.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

Privacy Officer
An official responsible for the coordination and implementation of all privacy and confidentiality efforts within a government department or component. This official may be statutorily mandated, as in the Department of Homeland Security, or appointed by a department or component to handle privacy and other related matters.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP108-109

GLOSSARY OF PRIVACY TERMS

Privacy Policy
An internal statement that governs an organization or entity’s handling practices of personal information. It is directed at the users of the personal information. A privacy policy instructs employees on the collection and the use of the data, as well as any specific rights the data subjects may have.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F11; US16-18

Privacy Policy in Standardized Machine-Readable Format
Defined by the U.S. Office of Management and Budget Memorandum M-03-22, “[a] statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.”

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G57, G67-68

Privacy Rule, The
Under HIPAA, this rule establishes U.S. national standards to protect individuals’ medical records and other personal health information and applies to health plans, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients’ rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US47-50, 134
Associated law(s): HIPAA

Private Right of Action
Unless otherwise restricted by law, any individual that is harmed by a violation of the law can file a lawsuit against the violator.

Associated term(s): Negligence
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US6

Professional Regulatory Body

IAPP Privacy Glossary, © 2012
Version 2.0.0.2
GLOSSARY OF PRIVACY TERMS

A body enacted pursuant to an act under which a professional or occupational group or discipline is organized and that provides for the membership in the regulation of the members of the professional or occupation group or discipline, including the registration, competence, conduct, practice and discipline of its members.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C34

Proportionality

Article 6(1)(c) of the Directive sets out the principle of proportionality: Member States shall provide that personal data must be: (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/ or further processed.

Applying the principle of proportionality entails a two-part assessment: (1) whether the means employed by the processing to be evaluated are suitable and reasonably likely to achieve the stated objectives; and (2) whether the adverse consequences that the processing has on an interest worthy of legal protection are justified in view of the importance of the objective pursued.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E87-89
Associated law(s): Data Protection Directive

Protected Health Information

Any individually identifiable health information transmitted or maintained in any form or medium that is held by a covered entity or its business associate; identifies the individual or offers a reasonable basis for identification; is created or received by a covered entity or an employer, and relates to a past, present or future physical or mental condition, provision of healthcare or payment for healthcare to that individual.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US46
Acronym(s): PHI

Protective Order

With a protective order, a judge determines what information should not be made public and what conditions apply to who may access the protected information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US128-130
Associated term(s): Redaction
**Public Key Infrastructure**
A system of digital certificates, authorities and other registration entities that verifies the authenticity of each party involved in an electronic transaction through the use of cryptography.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F96-97; IP184
Acronym(s): PKI
Associated term(s): Cryptography

**Public Law Enforcement Authorities**
A body sanctioned by local, regional or national government to enforce laws and apprehend those who break them. In Europe, public law enforcement authorities are governed by strict rules of criminal procedure designed to protect the fundamental human right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR).

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E227
Associated term(s): Law Enforcement Authority

**Public Records**
Information collected and maintained by a government entity and available to the general public.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F7, 71; IP7

**Publicity Given to Private Life**
A common law tort that states: “One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person and (b) is not of legitimate concern to the public.” (Restatement (Second) of Torts § 652D)

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US154-155
Associated term(s): Common Law
GLOSSARY OF PRIVACY TERMS

Publicly Available Information
Information that is generally available to a wide range of persons. Some traditional examples include names and addresses in telephone books and information published in newspapers or other public media. Today, search engines are a major source of publicly available information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F7; IP7

Purpose Limitation
This principle imposes limits on the processing of data for purposes other than those for which it was obtained.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E81
Associated term(s): Principle of Finality
Associated law(s): Data Protection Directive

Purpose Specification
A fair information practices principle, it is the principle stating that the purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F18, 22; IP12; E20, 253
Associated term(s): FIPs
Qualified Protective Order
Requires that the parties are prohibited from using or disclosing the Personal Healthcare Information (PHI) for any purpose other than the litigation and that the PHI will be returned or destroyed at the end of the litigation.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US134, 136

Acronym(s): QPO
Associated law(s): HIPAA
Associated terms: PHI


IAPP Privacy Glossary, © 2012
Version 2.0.0.2

GLOSSARY OF PRIVACY TERMS

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Radio-Frequency Identification
Technologies that use radio waves to identify people or objects carrying encoded microchips.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Acronym(s): RFID

Random Testing
Substance testing sometimes required by law, prohibited in certain jurisdictions, but acceptable where used on existing employees in specific, narrowly defined jobs, such as those in highly regulated industries where the employee has a severely diminished expectation of privacy or where testing is critical to public safety or national security.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US166
Associated term(s): Substance Testing

Real ID Act
An act aimed at promoting national security and reducing fraud that among, other things, established national standards for state-issued driver’s licenses and identification cards. Thus far, compliance deadlines for implementing the program have been extended and 25 states have passed resolutions to non-participate in the program.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G35-36

Reasonable Suspicion
A determining factor in substance testing where testing is allowed as a condition of continued employment if there is “reasonable suspicion” of drug or alcohol use based on specific facts as well as rational inferences from those facts; i.e., appearance, behavior, speech, odors.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US164-166
Associated term(s): Substance Testing
GLOSSARY OF PRIVACY TERMS

**Rectification**
Closely intertwined with access, rectification is the right or ability of a data subject to correct erroneous information that is stored about them. The right is provided by the EU Data Protection Directive and the American Fair Credit Reporting Act, among other laws.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP87-88; E90, 132-133
Associated term(s): Access
Associated law(s): Data Protection Directive; FCRA

**Redaction**
The practice of identifying and removing or blocking information from documents being produced pursuant to a discovery request or as evidence in a court proceeding. Specifically, attorneys are required to redact documents so that no more than the following information is included in court filings: (1) The last four digits of the Social Security number and taxpayer-identification number; (2) the year of the individual’s birth; (3) if the individual is a minor, only the minor’s initials, and (4) the last four digits of the financial account number.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US134-135
Associated term(s): Protective Orders

**Reidentification**
The process of using publicly available information to re-associate personally identifying information with data that has been anonymized.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Associated term(s): deidentification; anonymization

**Retention**
Within the information lifecycle the concept that organizations should retain personal information only as long as necessary to fulfill the stated purpose.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F16; IP173-174
Acronym(s):
Associated term(s):
Associated law(s):
Right Not To Be Subject to Fully Automated Decisions
Under Article 15 of the Data Protection Directive, individuals are entitled to object to being subject to fully automated decisions. The right, however, does not allow an individual to object to automated processing that then leads to a human decision.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E137
Associated law(s): Data Protection Directive

Right of Access
Generally, the right of individuals to obtain data about themselves from data controllers upon request. The right is accorded under Article 12 of the Data Protection Directive, although member states are afforded some latitude to implement the rule. In Canada, the right is provided by PIPEDA.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C76-77; E126

Right To Be Forgotten
A proposed right within the EU, with origins in French law, for individuals to remove information that they had given out about themselves. Proposed penalties for violations of the right could amount to up to two percent of a company's global income.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Associated term(s): le droit à l’oubli; right of oblivion

Right To Correct
The right for individuals to correct or amend information about themselves that is inaccurate.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C101

Right to Financial Privacy Act of 1978
GLOSSARY OF PRIVACY TERMS

Governs the release of customer financial information to federal government authorities. The act defines both the circumstances under which a financial institution can volunteer information about customers’ financial records to federal government authorities and the applicable procedures and requirements to follow when the federal government is requesting customers’ financial information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G31-33
Acronym(s): RFPA  x  x  x  x  C  x

Right to Object
A data subject’s ability to object to processing activities. The right to object is specifically defined in the EU Data Protection Directive, Article 14 and refers to two separate rights: A general right to object and a right to object to direct marketing.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E133-136

Right to Privacy, The
An 1890 law review article by Louis Brandeis and Samuel Warren arguing that privacy is the right to be left alone, and that the violation of this right should give rise to a tort.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F1; IP1, 26
Associated term(s): Right to be left alone  x  x  x  x  x

Right to Rectification, Erasure or Blocking
The right of subjects under the Data Processing Directive to request that a data processor remedy errors in data kept in regard to them.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E132-133
Associated term(s): Rectification; Erasure; Blocking  x  x  x  x  x  x

Risk Assessment Factors
The following constitute risk assessment factors: Number of breaches; number of outages; unauthorized access; lost assets; software viruses; investigations.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F80-81

IAPP Privacy Glossary, © 2012
Version 2.0.0.2
Role-Based Access Controls
Access policies that espouse the view that no employee should have greater information access than is necessary to capably perform his or her job function.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F94; IP177
Safe Harbor

The European Commission’s (EC) Directive on Data Protection (EC/46/95) prohibits the transfer of personal data to non-European Union nations that do not meet the European “adequacy” standard for privacy protection. While the U.S. and the European Union (EU) share the goal of privacy protection, the U.S. uses a sectoral approach that relies on a mix of legislation, regulation and self-regulation, while the EU 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 U.S. companies to engage in many trans-Atlantic transactions. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the directive, the U.S. Department of Commerce and the EC developed a “Safe Harbor” framework. The Safe Harbor—approved by the EU in 2001—is an important way for U.S. 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 a non-EU-based company provides adequate privacy protection, as defined by the directive. From a U.S. perspective, Safe Harbor is a self-regulatory regime that is only available to companies subject to the enforcement authority of the U.S. Federal Trade Commission or the U.S. Department of Transportation. Companies that are outside the jurisdiction of these two agencies are not eligible to join Safe Harbor.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E178-180

Sarbanes-Oxley Act

An example of a U.S. whistle-blower law, companies regulated by the law must establish a way for the company to confidentially receive and deal with complaints about actual or potential fraud from misappropriation of assets and/or material misstatements in financial reporting.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US159; E222-223

Acronym(s): SOX

Related term(s): Whistle-Blowing

Seal Programs

Programs that require participants to abide by codes of information practices and submit to monitoring to ensure compliance. In return, companies that abide by the terms of the seal program are allowed to display the programs seal on their website.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F33-34; IP5-6; US24; C5

Associated term(s): Self-regulatory Model, WebTrust

GLOSSARY OF PRIVACY TERMS

Secret Key
"A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities and which shall not be made public. The use of the term ‘secret’ in this context does not imply a classification level, rather the term implies the need to protect the key from disclosure or substitution.” (Federal Information Processing Standards Publication 140-1, Security Requirements for Cryptographic Modules)

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):

Sectoral Laws/Model
Laws that exist only in areas where the legislative body has found a particular need.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F32, 41-44; IP5; C5
Related term(s) Comprehensive Laws, Co-regulatory Model, Self-regulatory Model, Technology Based Model

Secure Sockets Layer
A protocol for establishing a secure connection for transmission that facilitates much of the online commerce that occurs on the Internet today. For example, HTTPS, a secure form of HTTP, is an SSL application used in password exchanges or e-commerce. “The primary goal of the SSL protocol is to provide privacy and reliability between two communicating applications.” The protocol has three main properties: (1) The connection is private; (2) the peer’s identity can be authenticated using asymmetric, or public key, cryptography, and (3) the connection is reliable.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F118, 124-125; IP201
Acronym(s): SSL
Related term(s) HTTP, HTTPS, TLS

Security Safeguards
A fair information practices principle, it is the principle that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

**Sedona Conference**

An important source of standards and best practices for managing electronic discovery compliance through data retention policies. Regarding e-mail retention, the Sedona Conference offers four key guidelines: (1) E-mail retention policies should be administered by interdisciplinary teams composed of participants across a diverse array of business units; (2) such teams should continually develop their understanding of the policies and practices in place and identify the gaps between policy and practice; (3) interdisciplinary teams should reach consensus as to policies while looking to industry standards; (4) technical solutions should meet and parallel the functional requirements of the organization.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US135

Associated term(s): Data retention, e-Discovery

**Self-Regulation Model, The**

Self-regulation refers to stakeholder-based models for ensuring privacy. The term “self-regulation” can refer to any or all of three pieces: legislation, enforcement and adjudication. Legislation refers to question of who defines privacy rules. For self-regulation, this typically occurs through the privacy policy of a company or other entity, or by an industry association. Enforcement refers to the question of who should initiate enforcement action. Actions may be brought by data protection authorities, other government agencies, industry code enforcement or, in some cases, the affected individuals. Finally, adjudication refers to the question of who should decide whether an organization has violated a privacy rule. The decision maker can be an industry association, a government agency or a judicial officer. These examples illustrate that the term “self-regulation” covers a broad range of institutional arrangements. For a clear understanding of data privacy responsibilities, privacy professionals should consider who defines the requirements, which organization brings enforcement action and who actually makes the judicial decisions.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F30, 33-34; IP5-6; US7; C5-6

Associated term(s): Comprehensive Laws, Co-regulatory Model, Online Privacy Alliance, Sectoral Laws, Self-Regulatory Model, Seal Programs, Technology Based Model

**Semayne’s Case**

A case recognized as establishing the "knock-and-announce rule," an important concept relating to privacy in one's home and Fourth Amendment search and seizure jurisprudence.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C2
**Senate (Canadian)**
One of two chambers of the Canadian Parliament, along with the House of Commons. Unlike the House of Commons, whose members are elected, the Senate is appointed by the governor in council based upon the recommendations of the prime minister.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C7
Associated term(s): Canadian Parliament, House of Commons

**Senior Agency Official for Privacy**
Under OMB Memorandum M-05-08, each executive agency should identify the senior official who has agency-wide responsibility for information privacy. The agency’s chief information officer (CIO) may perform this role, or it may be performed by another senior official at the assistant secretary or equivalent level. Agencies are also advised that the official given this role should have the authority to address information privacy policy issues at a national and agency-wide level. The official has overall responsibility and accountability for ensuring the agency’s implementation of information privacy protections, including full compliance with federal laws, regulations and policies relating to information security, such as the Privacy Act.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G91
Acronym(s): SAOP

**Sensitive Personal Information**
That which is more significantly related to the notion of a reasonable expectation of privacy. One’s medical or financial information is often considered sensitive personal information (SPI), but other types of personal information might be as well.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):
Acronym(s): SPI

**Six Major European Union Institutions, The**
The European Parliament, the European Council, the European Commission, the Court of Justice of the European Union, the European Central Bank and the Court of Auditors.
**Smart Grid**
An energy system that manages electricity consumption through continuous monitoring, remote computerization and automation. The traditional electric transmission system required physically sending workers into the field to periodically read customer meters and find where problems existed in the grid. Smart grid operators, however, can remotely monitor and control the use of electricity to each home or business.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E19-20

Associated term(s): Phishing

**Social Engineering**
A general term for how attackers can try to persuade a user to provide information or create some other sort of security vulnerability.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F119-120

**SPAM**
Unsolicited commercial e-mail.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F131-132; IP146; C128; E42-43, 265

Associated law(s): CASL; CAN-SPAM Act

**Special Categories of Data**
An EU term describing sensitive personal information, namely information pertaining to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F5; IP85; E100

GLOSSARY OF PRIVACY TERMS

Standard Model Clauses
Contractual agreements defined by the EU and Article 29 Working Party for the purpose of meeting the adequacy standards defined under the EU Data Protection Directive. Standard model clauses contain extensive data protection commitments and company liability requirements.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F37; IP251; E293-294
Acronym(s): SMCs

Stored Communications Act
The Stored Communications Act (SCA) was enacted as part of Electronic Communications Privacy Act in 1986. It generally prohibits the unauthorized acquisition, alteration or blocking of electronic communications while in electronic storage in a facility through which an electronic communications service is provided.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US143, 169
Acronym(s): SCA
Associated law(s): The Electronic Communications Privacy Act of 1986 (ECPA)

Subpoena
A written court order issued in an administrative, civil or criminal action that requires the person named in the subpoena to appear in court in order to testify under oath on a particular matter which is the subject of an investigation, proceeding or lawsuit. A subpoena may also require the production of a paper, document or other object relevant to an investigation, proceeding or lawsuit that discloses personal information.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP77-78; G31

Substance Testing
A screening to identify drug use. Substance testing can be used in a variety of settings such as preemployment, reasonable suspicion, routine testing, post-accident testing or randomly.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US165-166
Associated terms(s): Americans with Disabilities Act, Random Testing, ReasonableSuspicion


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
**Substitute Notice**

Most legislation recognizes that data breach notifications involving thousands of impacted data subjects could place an undue financial burden on the organization and therefore allow substitute notification methods. In Connecticut, for example, "Substitute notice shall consist of the following: (A) Electronic mail notice when the person, business or agency has an electronic mail address for the affected persons; (B) conspicuous posting of the notice on the website of the person, business or agency if the person maintains one, and (C) notification to major state-wide media, including newspapers, radio and television."

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US123

Associated term(s): [Data Breach](#)

**Syndicated Content**

Content that is not actually created by the host site, but is developed, purchased or licensed from a third party. A concern associated with this content is that it can contain malicious code that is then unwittingly incorporated into the organization’s own website source code. For example, cross-site scripting (XSS) attacks attempt to take advantage of the trust that users have for a given site.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F129; IP205

Associated term(s): [XSS](#)

**System of Records Notice**

A notice required when a federal agency creates, modifies or destroys a system of records. When the agency collects and stores Personally Identifiable Information in records, the agency is required to establish the statutory need for the collection, disclose the collection, describe its contents and declare the routine uses for that agency or any other agency that will use the information. This disclosure must be made to the Office of Management and Budget and Congress and must be published in the *Federal Register* in advance of the system becoming operational.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G50

Acronym(s): [SORN](#)

Associated law(s): [Privacy Act, The](#)
**Technology-Based Model**

The technology-based model for data protection utilizes technological security measures to protect individuals’ personal data. While it is commonplace for companies to utilize technology to protect data, developments in commercially available hardware and software have enabled consumers to establish privacy protections for their own online activity.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F34; IP6; C6-7

Associated term(s): Comprehensive Laws, Co-regulatory Model, Sectoral Laws, Self-Regulatory Model

---

**Territorial Privacy**

One of the four classes of privacy, along with information privacy, bodily privacy and communications privacy. It is concerned with placing limitations on the ability of one to intrude into another individual’s environment. Environment is not limited to the home; it may be defined as the workplace or public space and environmental considerations can be extended to an international level. Invasion into an individual’s territorial privacy typically comes in the form of video surveillance, ID checks and use of similar technology and procedures.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F2; IP2, C2

Associated term(s): Home Privacy

---

**Traffic Data**

This refers to any data processed for the purpose of the conveyance of a communication on an Electronic Communications Network or for the billing thereof. Traffic data includes information about the type, format, time, duration, origin, destination, routing, protocol used and the originating and terminating network of a communication. For example, in relation to a telephone call, traffic data includes, among other information, the phone numbers of the caller and call recipient; in relation to an e-mail, the e-mail addresses of the sender and recipient’ and the size of any attachments.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E229

---

**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.
GLOSSARY OF PRIVACY TERMS

Transit
The automatic forwarding of data packets from one server to another.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E75, 174

Transmission Control Protocol
A protocol which enables two devices to establish a connection and exchange data. A combination of TCP and IP is used to send data over the Internet. Data are sent in the form of a packet, which is a portion of a message sent over the TCP/IP network. It contains content and a heading that specifies the destination.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F118; IP201
Acronym(s): TCP; TCP/IP

Transparency
The requirement to be open and honest about manner in, and purposes for, which personal data is used. It is a fundamental principle in privacy protections and a key concept of the European data protection framework.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E107-111

Transport Layer Security
A protocol that ensures privacy between client-server applications and Internet users of the applications. When a server and client communicate, TLS secures the connection to ensure that no third party can eavesdrop on or corrupt the message. TLS is a successor to SSL.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F118, 124-125
Acronym(s): TLS
Associated term(s): Secure Sockets Layer (SSL)
GLOSSARY OF PRIVACY TERMS

**Treaty of Lisbon**
Signed in 2007, and effective in 2009, its main aim was to strengthen and improve the core structures of the European Union to enable it to function more efficiently. The Lisbon Treaty amends the EU’s two core treaties, the Treaty on European Union and the Treaty Establishing the European Community. The treaty ensures that all institutions of the European Union must protect individuals when processing personal data. It also established a European Data Protection Supervisor whose role is to regulate compliance with data protection law within the institutions of the European Union, but its references to “authorities” implies that the national data protection authorities may also have jurisdiction in such matters.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E14-19
Associated term(s): Lisbon, EDPS

**Trojan Horse**
A form of malware in which bad software masquerades as beneficial software.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F99
Associated term(s): Malware

---


IAPP Privacy Glossary, © 2012
Version 2.0.0.2
U.S. Department of Labor
A U.S. federal agency that oversees “the welfare of the job seekers, wage earners and retirees of the United States by improving their working conditions, advancing their opportunities for profitable employment, protecting their retirement and healthcare benefits, helping employers find workers, strengthening free collective bargaining and tracking changes in employment, prices and other national economic measurements.” To achieve this mission, the department administers a variety of federal laws including, but not limited to, the Fair Labor Standards Act (FLSA), the Occupational Safety and Health Act (OSHA) and the Employee Retirement Income Security Act (ERISA).
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US157

Unambiguous Consent
Generally, it is consent that is given as part of a positive and definite act where there is no doubt that consent has been given. Under EU Directives, the term is defined under member state laws.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): E94

Unfair Trade Practices
Commercial conduct that intentionally causes substantial injury, without offsetting benefits, and that consumers cannot reasonably avoid.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP70; US18-20

Uniform Resource Locator
The address of content located on a web server. Specifically, it is the letter and number coordinates that an end user submits to the web browser to instruct it to connect with the desired website. An example of a URL is “http://www.privacyassociation.org.”
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F131-132; IP200

Acronym(s):
- URL
**GLOSSARY OF PRIVACY TERMS**

**Associated term(s):** Domain Name

**United States Department of Health, Education and Welfare Fair Information Practice Principles (1973), The**

A code of fair information practices that contained five principles: (1) There must be no personal data record keeping systems whose very existence is secret. (2) There must be a way for an individual to find out what information about him (or her) is in a record and how it is used. (3) There must be a way for an individual to prevent information about him (or her) that was obtained for one purpose from being used or made available for other purposes without his (or her) consent. (4) There must be a way for an individual to correct or amend a record of identifiable information about him (or her). (5) Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP27; G5-6

**Associated term(s):** HEW Principles; HEW Report, The

**Universal Declaration of Human Rights**

Also called the Human Rights Declaration, the declaration recognized the universal values and traditions of inherent dignity, freedom, justice and peace. It was adopted by the General Assembly of the United Nations on 10 December 1948. In December 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights. This declaration formally announced that “[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence” The statement was intended to encompass a wide range of conduct, as evidenced by Article 12 of the Declaration, which describes both the territorial and the communications notions of privacy.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F3; IP2; C2-3; E4, 15

**Associated term(s):** Declaration of Human Rights

**USA-PATRIOT Act**

A broad-ranging act designed to counter terrorism that expanded law enforcement authority to surveillance and capturing communications and records.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP 75; US74, 132, 148; C88-90; G34-35

**Acronym(s):** USAPA

**Associated term(s):** Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; Patriot Act

US-CERT
A partnership between the Department of Homeland Security and the public and private sectors intended to coordinate the response to security threats from the Internet. As such, it releases information about current security issues, vulnerabilities and exploits via the National Cyber Alert System and works with software vendors to create patches for security vulnerabilities.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): G95-96
Acronym(s): US-CERT
Associated term(s): U.S. Computer Emergency Readiness Team

Use Limitation
A fair information practices principle, it is the principle that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 8 of the Fair Information Practice Principles except with the consent of the data subject or by the authority of law.
Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F18, 20; IP12; C19; E232-233, 260; G7
Associated term(s): Fair Information Practices
Value-Added Services
A telecommunications industry term for non-core services; i.e., services beyond voice calls and fax transmissions. More broadly, the term is used in the service sector to refer to services, which are available at little or no cost, and promote their primary business. For mobile phones, while technologies like SMS, MMS and GPRS are usually considered value-added services, a distinction may also be made between standard (peer-to-peer) content and premium-charged content. These are called mobile value-added services (MVAS), which are often simply referred to as VAS. Value-added services are supplied either in-house by the mobile network operator themselves or by a third-party value-added service provider (VASP), also known as a content provider (CP) such as All Headline News or Reuters. VASPs typically connect to the operator using protocols like short message peer-to-peer protocol (SMPP), connecting either directly to the short message service centre (SMSC) or, increasingly, to a messaging gateway that gives the operator better control of the content.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP96; C117; E232-233, 260
Associated term(s): MVAS, VASP

Video Surveillance
Recordings that do not have sound.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): US168-169
Associated term(s): Video Surveillance Guidelines
Associated law(s): FISA

Video Surveillance Guidelines
Guidelines discouraging video as an initial security option with the following constraints: (1) Video should be taken only in the absence of less intrusive alternatives; (2) the use should be disclosed to the public; (3) individuals should have access to their personal information; (4) video surveillance should be subject to independent audit, and (5) fair information practices should be respected.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C81

Virtual Private Network
A network that uses primarily public telecommunication infrastructure, such as the Internet, to provide...
remote offices or traveling users an access to a central organizational network. VPNs typically require remote users of the network to be authenticated and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F87; IP168
Acronym(s): VPN
Associated term(s): Remote Access Connectivity

Voice Over Internet Protocol
A technology that allows telephone calls to be made over a LAN or the Internet itself. Skype is a well-known example. VoIP poses the same risk as network-connected PBX systems but also poses the additional risk of data interception when such data travel over an unsecured connection. VoIP functionality should be encrypted where possible and equipment monitored with intrusion-detection systems.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): F88; US100; IP169
Acronym(s): VoIP
Web Beacon
Also known as a web bug, pixel tag or clear GIF, a web beacon is a clear graphic image (typically one pixel in size) that is delivered through a web browser or HTML e-mail. The web beacon operates as a tag that records an end user’s visit to a particular web page or viewing of a particular e-mail. It is also often used in conjunction with a web cookie and provided as part of a third-party tracking service. Web beacons provide an ability to produce specific profiles of user behavior in combination with web server logs. Common usage scenarios for web beacons include online ad impression counting, file download monitoring, and ad campaign performance management. Web beacons also can report to the sender about which e-mails are read by recipients. Privacy considerations for web beacons are similar to those for cookies. Some sort of notice is important because the clear pixel of a web beacon is quite literally invisible to the end user.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F138; IP217; G66
Associated term(s):  Web Bug, Pixel Tag, Tracking Bug, Clear GIF

WebTrust
Created by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). It is a self-regulating seal program which licenses qualifying certified public accountants.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  F34; IP6
Associated term(s):  Seal Programs

Whistle-Blowing
The reporting of illegal or improper actions within a company by an employee of said company.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page):  IP118; US156; E223-225
Associated term(s):  Whistleblowing; Whistleblower
Associated law(s):  SOX

Wide Area Network
A non-localized telecommunications network that can be used to transmit data across large regions.
**Work Product Information**

A Canadian term referring to information about an individual that is related to that individual’s position, functions and/or performance of his or her job. A term that is undefined by PIPEDA, the privacy commissioner has decided that work product may at times fall under the definition of personal information. Access to such information by the commissioner is addressed on a case-by-case basis. Not to be confused with the American legal term "work product," which refers to legal materials prepared in anticipation of litigation.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): C17; 32-33
Associated term(s): Employee Information
Associated law(s): PIPEDA

**Works Councils**

Bodies that represent employees and have certain rights under local law that affect the use of employee data by employers. Their power varies widely by jurisdiction.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP132; E221-222
Associated term(s): Labor Unions; Unions; Labour Unions

**Worm**

A computer program or algorithm that replicates itself over a computer network, usually performing malicious actions.

Reference(s) in IAPP Certification Textbooks (see key at bottom of page): IP202
Associated term(s): Flash Worm
GLOSSARY OF PRIVACY TERMS

CF = Certification Foundation
US = CIPP/United States (private sector)
CA = CIPP/Canada
EU = CIPP/Europe
Gov = CIPP/Government (United States)
IT = CIPP/Information Technology


IAPP Privacy Glossary, © 2012
Version 2.0.0.2