Glossary B -
Terms and Organizations Related to
Internet Privacy Regulatory Framework

(Note: The source for the definition is identified in parentheses following the definition.)

* IAPP is the International Association of Privacy Professionals

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. (IAPP)

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. (IAPP)

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. (IAPP)

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. (IAPP)

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. (IAPP)

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. (IAPP)

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. (IAPP)

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. (IAPP)

Children's Online Privacy Protection Act of 2000, The - (COPPA). 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. (IAPP)

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. (IAPP)

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. (IAPP)

Cookie Directive - Related to the EU-U.S. Safe Harbor and subsequent Privacy Shield framework. Refers to an EU 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. (IAPP)

COPPA Rule - An FTC rule that requires websites and apps to get parental consent before collecting personal information from kids under 13. The Rule was revised in 2013 to strengthen kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13. (FTC)

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. (IAPP)

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. (IAPP)

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. (IAPP)

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. (IAPP)

Disposal Rule - An FTC rule under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the Fair Credit Reporting Act (FCRA), requires that companies dispose of credit reports and information derived from them in a safe and secure manner. (IAPP)

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. (IAPP)

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. (IAPP)

Electronic Communications Privacy Act of 1986 - The collective name of the U.S. 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. (IAPP)

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. (IAPP)

European Council - A forum where heads of state meet four times a year to define priorities and set political direction for the EU. (IAPP)

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. (IAPP)

European Union - The European Union (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. (IAPP)

Fair Information Practice Principles - The U.S. Federal Trade Commission Information Practice Principles (FIPP). Guidelines that represent widely accepted concepts and standards concerning fair information practices in an electronic market Place. (Wikipedia) The principles are:

- Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).

- Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

- Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

- Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

- Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

- Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

- Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements. (NSTIC)

Federal Trade Commission (FTC) - An independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models. (FTC website)

Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999. Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. (FTC website)

Health Breach Notification Rule - An FTC rule that requires certain Web-based businesses to notify consumers when the security of their electronic health information is breached. (FTC website)

National Strategy for Trusted Identities in Cyberspace (NSTIC) - A White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions.

Non-Public Personal Information - Defined by U.S. Gramm-Leach-Bliley Act as personally identifiable financial information that is: (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. Does not include: (i) publicly available information or (ii) any consumer list that is derived without using personally identifiable financial information. (IAPP)

Personal Information or Personal Identifying Information (PII) - 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 physical, physiological, mental, economic, cultural or social identity. (IAPP)

Privacy of Consumer Financial Information Rule. An FTC rule under the GLBA that required financial institutions covered by the Gramm-Leach-Bliley Act must tell their customers about their information-sharing practices and explain to customers their right to "opt out" if they don't want their information shared with certain third parties. (FTC website)

Privacy Rule - 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. (IAPP)

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. (IAPP)

Privacy Shield - Successor to EU-U.S. Safe Harbor agreement. A mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. To join the Privacy Shield Framework, a U.S.-based company will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield Framework will be voluntary, once an eligible company makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. (U.S. Dept. of Commerce website)

Protected Health Information (PHI)- Under U.S. HIPAA law, any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual. (Wikipedia)

Red Flags Rule - An FTC rule that requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

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. (IAPP)

Safe Harbor - Recently replaced by the Privacy Shield. 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. (IAPP)

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. (IAPP)

Sensitive Personal Information - Any information that could be used by criminals to conduct identity theft, blackmail, stalking, or other crimes against an individual.