Glossary A -
Basic Terms Related to the Internet

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

Add-on, Plug-in, or Add-in - A software product designed to enhance another software product. It usually cannot be run independently. (multiple)

Adware - Software that performs certain functions for advertisers, such as sending an ad to a specific website when it is being visited by the consumer that is being tracked by the adware. Adware may be installed on a computer as part of a bundle of software that a consumer purchases, or it may be embedded into a free download. (multiple)

Analytics - The discovery, interpretation, and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance. Firms may apply analytics to business data to describe, predict, and improve business performance. (Wikipedia)

App - A Web application (Web app) is an application program that is stored on a remote server and delivered over the Internet through a browser interface. (TechTarget)

Algorithm - In mathematics and computer science, an algorithm (e.g., Listeni/'ælg?r?ð?m/ AL-g?-ri-dh?m) is a self-contained step-by-step set of operational instructions to perform a calculation, data processing, and automated reasoning. A computer algorithm is basically an instance of logic written in software by software developers to be effective for the intended "target" computer to produce output from given input. (Wikipedia) Algorithms are used by the behavioral advertising industry to profile consumers.

Beacon or Web Beacon - Also known as a bug, pixel tag, or clear GIF. A clear graphic image (typically one pixel in size) that is delivered through a browser or HTML e-mail. It records an end user's visit to a particular web page or viewing of a particular e-mail. Often used in conjunction with a cookie and used to provide for third-party tracking. Allows specific profiles to be made of user online behavior in combination with web server logs. Certain beacons can report to the sender about which e-mails are read by recipients. Privacy considerations for web beacons are similar to those for cookies. Invisible to the end user. (International Association of Privacy Professionals - IAPP)

Behavioral Advertising - The act of tracking users' online activities and then delivering ads or recommendations based upon the tracked activities. (IAPP)

Breach - The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector. (IAPP)

Browser - Software program that allows a person to search for and view various kinds of information on the Web. For example, Internet Explorer, Google Chrome, Yahoo!, Bing, and Firefox. (About.com)

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. (IAPP)

Cloud - Software and services that run on the Internet instead of your computer, for example, Apple iCloud, Dropbox, Netflix, Amazon Cloud Drive, Flickr, Google Drive, Microsoft Office 365, Yahoo Mail. (CNN Money) When something is in the cloud, it means it is stored on servers on the Internet instead of on your computer. It lets you access your calendar, email, files, and more from any computer that has an Internet connection. (GCF LearnFree.org)

Cookie - 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. Also used to prevent users from having to be authorized for every password protected page they access during a session by recording that they have already successfully supplied their user name and password. May be referred to as "first-party" cookeis (if they are placed by the website that is visited) or "third-party" cookies (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. (IAPP)

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

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

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. (IAPP)

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

Digital Fingerprinting - The use of web log files to identify a website visitor. 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. (IAPP)

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. (IAPP)

Firewall - A network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. (TechTarget)

Hacker - A person who uses computers to gain unauthorized access to data. (multiple)

Hard drive - Also known as a hard disk drive (HDD), is a fundamental part of modern computers. It allows a computer to house and execute important files and programs, like the machine's operating system, and its components work together to actively seek, read, and write data on system and user-generated files. There are two main types of hard drives: internal and external. The internal hard drive is where the fundamental programs are stored. (multiple)

HTML - Hypertext Markup Language. A content authoring language used to create web pages. Browsers use HTML to interpret and render visible and audible content on web pages. Document “tags” can be used to format and lay out web page content and to “hyperlink”—connect dynamically—to other web content. (IAPP)

http - Hypertext Transfer Protocol. A networking language that manages data packets over the Internet. It defines how messages are formatted and transmitted and defines what actions servers and browsers take in response to various commands. (IAPP)

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. (IAPP)

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. (IAPP)

Internet - The global system of interconnected mainframe, personal, and wireless computer networks that use the Internet protocol suite (TCP/IP) to link billions of electronic devices worldwide. (Wikipedia)

Intrusion Detection System - IDS. A system that inspects network activity and identifies suspicious patterns that maybe 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. (IAPP)

Intrusion Prevention System (IPS) - 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. (IAPP)

IP Address - Internet Protocol Address. A unique string of numbers that identifies a computer on the Internet or network. The IP address is expressed in four groups of up to three numbers, separated by periods. For example: 123.123.23.2. May be "dynamic," meaning that it is assigned temporarily whenever a device logs on to a network and so it changes each time a device connects. Or, may be "static," meaning that it is assigned to a particular device and does not change, but remains assigned to one computer or device. (IAPP)

Javascript - A computer scripting language used to produce interactive and dynamic web content. (IAPP)

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. Used to identify the real-world geographic location of computer, cell phone, or other device. (IAPP)

Malware - Unwanted or maliciously installed software. A computer virus is a type of malware that replicates itself and spreads within the user's computer like an infection. (multiple)

Opt-In - One of two central concepts of choice. It means an individual makes an active affirmative indication of choice, e.g., checking a box to signal consent share information with third parties. (IAPP)

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. (IAPP)

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, beacons, or other types of identification mechanisms. (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)

Personal Information Banks (PIBs) - Personal information that is organized or intended to be retrievable by a person's name or by a number, symbol, or other identifier assigned only to that person. (multiple)

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 someone the user knows and that instructs the user to provide information. (IAPP)

Pixel tag - See Beacon.

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

SSL - See TSL/SSL.

Server Log - Information automatically recorded by a data server when a website is visited. Typically include a users web request, Internet Protocol address, browser type, browser language, the date and time of the request and one or more cookies that may uniquely identify the user's browser. (Wikipedia)

Software - Organized computer program information, such as operating systems, utilities, and applications that enable computers to work. Consists of instructions and code written by programmers in any of various special computer languages. Commonly divided into two main categories: (1) system software, which is invisible to the user and controls the basic functions of a computer and is usually preinstalled with the machine; and (2) application software, which handles common and specialized tasks that a user wants to perform, such as accounting, communicating, data processing, word processing. (BusinessDictionary.com)

SPAM - Unsolicited commercial e-mail. (IAPP)

Spyware - A type of software that gathers personal information without the individual's knowledge or consent. Some spyware asserts control over a computer without the consumer's knowledge. (multiple)

TLS/SSL - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). Cryptographic protocols designed to provide communications security over a computer network. (Wikipedia)

Syndicated Content - The process of pushing content out and onto third-party websites, either as a full article, snippet, link, or thumbnail. (multiple)

Transmission Control Protocol (TCP)- Code that enables two devices to establish a connection and exchange data. (IAPP)

Trojan Horse - A form of malware in which the software masquerades as beneficial software. (IAPP)

Virus - A piece of computer code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. (multiple)

Web or World Wide Web (www) - A system of Internet servers that supports specially formatted documents. The documents are formatted in a markup language called HTML (HyperText Markup Language) that supports links to other documents (i.e, web page), as well as graphics, audio, and video files. Not all Internet servers are part of the Web. (webopedia)

Worm - A type of computer virus that is a program or algorithm that replicates itself over a computer network, usually performing malicious actions. (IAPP)