

THE ANONOPEDIA

The Anonopedia is a glossary of key terms and concepts related to privacy, anonymity and identity. Written in simple, ordinary language, its purpose is to provide readers with a greater understanding of privacy related topics by removing disciplinary barriers that technical or professional terms might otherwise present.

The Anonopedia was developed collaboratively by Stephanie Perrin, who, prior to heading up the research and policy branch of the Office of the Privacy Commissioner of Canada, was the Project's Research Co-ordinator, and two of the projects partners, [CIPPIC](#) (under the direction of Pippa Lawson, Executive Director and General Counsel) and [EPIC](#) (under the direction of Chris Hoffnagle, Director and Senior Counsel, EPIC West). The Anonopedia represents the work of many of the project's students who have developed definitions and links to resources, and we would like to thank the following for their work: Jennifer Barrigar, Erin Callery, Uruszula Galster, Michelle Gordon, Carole Lucock, and Leila Pourtavaf. We would also like to thank Professor Elizabeth Judge, Faculty of Law, University of Ottawa for her assistance with this project.

The Anonopedia should be read as a work-in-progress and will be updated from time to time with additions or revised definitions. Consequently, we encourage you to submit suggested terms to add to the Anonopedia (for example, a term that you searched for and were unable to find; we also welcome proposed definitions).

Contact: contact@anonequity.org

Access Management:

The maintenance of all access information used to grant users access to certain resources. It consists of four tasks: account administration, maintenance, monitoring, and revocation.

Resources:

<http://64.233.161.104/search?q=cache:rizCsCipOgEJ:www.2ab.com/pdf/AccessManagement.pdf+define+access+management&hl=en>

http://business.cisco.com/glossary/tree.taf-asset_id=92870&word=103623&public_view=true&kbns=2&DefMode=.htm

ActiveX Control:

A program that lets web browsers download and use Windows programs. For example, "Netscape Communicator's support for ActiveX allows users to open an Excel spreadsheet from within Netscape Navigator."¹ ActiveX controls have been shown to pose a number of security risks to users. One of the major problems with ActiveX controls is that they can automatically download and execute potentially hostile programs from a web site. The downloaded program could then access or damage the data on the machine through, for example, inserting a virus.

Reference:

1. <http://about-the-web.com/shtml/glossary.shtml>

Other Resources:

<http://www.cs.princeton.edu/sip/java-vs-activex.html>

<http://www.infoweblinks.com/content/activex.htm>

<http://www.iseran.com/ActiveX/>

Ad-blocker:

Ad-blocker is software which improves browser performance and usability by blocking ads while you are browsing the Web. While Ad-blockers have been around for several years, they are still only used by a relatively small percentage of internet users.

Ad-blockers were initially introduced by independent software companies. However, currently, many major software companies have integrated ad-filtering and blocking technologies into popular application suites. One major

advantage of Ad-blockers is that they speed up downloading time through eliminating slow-loading banners and buttons.

However, some argue that blocking ads is a form of theft since ad-free users can access valuable resources while avoiding “paying” in the form of viewing the ads which generate the revenue of the resource.

Resources:

http://www.marketingterms.com/dictionary/ad_blocking/

<http://www.intermute.com/adsubtract/>

<http://www.guidescope.com/home/>

Adware:

Any software application that displays advertising banners (generally through pop-up windows or bars) while the program is running. Some argue that Adware is a good way for companies to generate income, which in turn helps recover programming development cost and keeps the cost down for the user. Critics, however, believe that Adware usually includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. This practice has been dubbed spyware and has prompted an outcry from computer security and privacy advocates, including the Electronic Privacy Information Center (EPIC).¹

A number of software applications and ad-blockers have been developed (including Ad-Aware and OptOut) to help computer users search for and remove suspected spyware programs.

See also: **spyware**

Reference:

1. <http://www.epic.org>

Other Resources:

http://whatis.techtarget.com/definition/0,289893,sid9_gci521293,00.html

<http://cexx.org/problem.htm>

<http://searchsecurity.techtarget.com>

Anonymizer:

A privacy service that allows users to visit Web sites anonymously so that the sites cannot gather information (including IP address, browser and operating system identification, and cookie-stored data) from the user. Anonymizers often work like firewalls: when the user clicks on a hyperlink or types a URL, the anonymizing server intervenes and gets the information for the user. The Web site which is being viewed only receives information about the anonymizer, not the user machine. While the anonymizer protects the user's privacy on the Internet, it also prevents the site from tailoring their content for specific users and users have to re-enter personal identification when re-visiting a site.

Resources:

<http://www.computerworld.com/securitytopics/security/story/0,10801,91170,00.html>

<http://anonymizer.com/>

Authentication (See also authenticity, authentication technologies, authorization, and electronic authorization):

Authentication is a process that attests to the identity of an individual, process or device through the use of cryptographic and physical data. Authentication usually relies on data such as user names and passwords, digital signatures, biometric identifiers and smart cards. As the use of electronic communications grows from searching for information, to exchange of personal data and money, there is a greater need for the security and privacy of online communications and transactions. The purpose of authentication is to ensure maximum security in electronic communication.

Resources:

<http://www.webopedia.com/TERM/a/authentication.html>

http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00240e.html

<http://www.oecd.org>

Audit Trail:

A record that tracks computer activity showing who has accessed a computer system, as well as the period of time the system was accessed and the operations that were performed during the visit. An audit trail's primary function is to allow for the recovery of lost data and to provide some security. Most accounting systems and database management systems include an audit trail component. In addition, there are separate audit trail

software products for network administrators which allow them to monitor the use of their network. There are different kinds of audit trails including:

- **Accounting audit trails** are usually paper trails that confirm the validity of accounting entries.
- **Computing audit trails** are usually electronic logs that track computer activity.
- **E-commerce audit trails** are used to record and monitor customer activities in order to respond to inquiries, complaints, as well as to record sales.
- **Criminal investigations** use audit trails to investigate crimes (especially cyber crimes).

Resources:

http://www.webopedia.com/TERM/A/audit_trail.html

http://en.wikipedia.org/wiki/Audit_trail

http://whatis.techtarget.com/definition/0,289893,sid9_gci541384,00.html

Authorization :

Authorization is the process of granting a subject access to certain information, services, and resources. Authorization usually relies on an authentication process that confirms the identity of the person, computer process, or device before allowing the subject access to the request.

Resource:

<http://www.webopedia.com/TERM/a/authorization.html>

Automated Fingerprint Identification System (AFIS):

AFIS is an identification method that uses biometrics. Relying on digital imaging technology AFIS obtains, stores, and analyzes fingerprint data. The technology was originally developed over 25 years ago for use by law enforcement agencies such as the FBI to compare an individual's fingerprint with a database of fingerprint images. Current developments have allowed for governmental and commercial applications of the technology. In particular, recent government programs aimed at controlling national security, terrorist activity and border and immigration control have created a large and expanding market for AFIS. While the method gained favor for general identification purposes and fraud prevention, it has also been criticized by privacy and civil liberties advocates.

Resources:

<http://www.findbiometrics.com/Pages/glossary.html>

http://www.bioprivacy.org/faq_main.htm

<http://www.privacyrights.org/ar/Privacy-IssuesList.htm#A>

Automatic Identification and Data Capture/Collection (AIDC):

AIDC is a general term for the process of collecting information through automatic means. RFID, bar code scanning, biometrics, smartcards, and OCR all fall under the category of AIDC.

Resource:

<http://www.webopedia.com/TERM/A/AIDC.html>

Automated Information System (AIS):

AIS is a general term for systems such as computers, word processing software, networks, or other electronic information handling systems, and associated equipment. AIS is a combination of computer hardware and software, data, and telecommunications, information technology, and other resources that perform administrative functions such as collecting, recording, processing, transmitting, retrieving, storing, and displaying information. AIS does not include computer hardware and software that are a part of the research, development and use of weapon systems.

Resource:

<http://www.nap.edu/books/0309055970/html/88.html>

Bots:

Short for robot, a bot is a computer program that runs automatically and operates as an agent for a user, another program or to simulate a human activity. There are several kinds of bots, but the most common Internet bots are called spiders or crawlers that access Web sites and gather their content for search engine indexes.

Resources:

http://whatis.techtarget.com/definition/0,289893,sid9_gci211699,00.html

<http://www.botspot.com/>

Cache:

The place in a hard drive where the Web browser stores information (text, audio, graphics, etc.) about recently visited sites and pages. The storage of such information allows the user faster and easier access to the sites in the future because when re-visiting them, the browser compares the cached copy of the site to its original. If there are no changes between the two versions, rather than reloading the site onto the user's computer, the browser refers to the cached copy thereby saving downloading and processing time. The term also refers to a Web site's database which generates static copies of frequently requested dynamic pages, which also reduces processing time.

Resources:

<http://www.consumerprivacyguide.org/glossary/>

<http://about-the-web.com/shtml/glossary.shtml>

Carnivore [DCS 1000]:

Carnivore, now referred to as DCS 1000, is an email surveillance tool developed for the United States Federal Bureau of Investigation (FBI). Carnivore involves the installation of a computer system at an Internet Service Provider (ISP) either with permission or in response to a warrant. The computer system captures and analyzes communications data, looking for messages in transit that match a particular set of filtering criteria (for instance a particular sender or recipient, a particular type of transaction, etc.). When such a match occurs, the message as well as information on the date, time, origin and destination is logged and provided to the FBI. While the system was originally named to convey the idea that it only picked out the "meat" of the data flow, FBI documents showed that the system captures all communications, and filters the messages for delivery to law enforcement.

See also: **Internet Service Provider; Packet Sniffer; Filter**

Resources:

[http://en.wikipedia.org/wiki/Carnivore_\(FBI\)](http://en.wikipedia.org/wiki/Carnivore_(FBI))

<http://www.itsecurity.com/dictionary/carnivore.htm>

http://www.theregister.co.uk/2000/12/19/how_carnivore_works/

http://www.usdoj.gov/jmd/publications/carniv_final.pdf

http://www.epic.org/privacy/carnivore/foia_documents.html

Challenge and response:

Challenge and response is a commonly used authentication technique where an individual is asked to provide private information in order to gain access. Challenge and response is often used for security systems that rely on smart cards. A user is given a code (the challenge) which he or she enters into the smart card. In return, the smart card displays a new code (the response) with which the user can log in.

Resource:

http://www.webopedia.com/TERM/C/challenge_response.html

Chief Privacy Officer (CPO):

The CPO is the person inside an organization or company who is responsible for administering privacy law, privacy policy and privacy practices. In Canada, as in certain European privacy legislation, the position is mandated by law (i.e. an organization must name someone to be accountable).

While there is no precise definition of the role of a CPO, some responsibilities of the position include:

- Tracking pending legislation
- Staying up-to-date on new technologies
- Ensuring via direct contact with senior management that their company's strategic efforts are in alignment with such developments.

Former Microsoft CPO Richard Purcell says that the CPO position "represents a transition to an active corporate stance on privacy. It is no longer a case of defensive risk management, but recognition that privacy is a product that establishes our organisation's credibility and trust with consumers and society."¹ There are now numerous professional associations of CPOs including International Association of Privacy Professionals (IAPP).

Reference:

1. Purcell, Richard, "CPO Sharpies," CFRO: The Magazine for Senior Financial Executives, September, 2000.

Other Resources:

<http://www.pwcglobal.com/extweb/newcolth.nsf/0/732AC589FCF6A523852569BD005A07CB?OpenDocument>

http://www.privacyassociation.org/html/about_iapp.html
<http://www.computerbytesman.com/>

Click stream data:

Click stream data is a virtual trail of a user's activities while browsing the Internet. A click stream records information such as the Web sites and every page of those sites that the user visits, how long the user visited the page or site, in what order the pages were visited, any newsgroups in which the user participates and even the e-mail addresses to which the user sent or from which the user received messages. Click Stream Information is associated with the computer browser and not with an individual personally. Both ISPs and individual Web sites are capable of tracking a user's click stream. The data gathered is becoming increasingly valuable to Internet marketers and advertisers.

Resources:

<http://www.webopedia.com/TERM/C/clickstream.html>

<http://www.cdma.org/newethisc.html>

Client-based filter:

A software program that runs on a user's machine in order to block certain Internet communications, such as: blocking access to pornographic Web sites, preventing children from accessing the Internet at certain times, or preventing children from revealing personal information to others over the Internet. The filter is responsible for rejecting inappropriate materials before they are passed through the server.

See also: **Filter**

Resources:

<http://www.internet-filters.net/info.html>

<http://www.getnetwise.org/glossary>

<http://www.peacefire.org/>

Clipper Chip:

The Clipper Chip was a proposal for "key escrow encryption," a system for secure Internet communication where the government retained a key that allowed access to the messages. The clipper chip became famous because it incorporated a purportedly unbreakable algorithm (named skipjack) developed and controlled by the United States government. The United States government further proposed that Clipper Chip use be required for all encrypted communications and that the government retain control over the algorithm and access to any communications using the Clipper Chip. Significant lobbying from privacy and civil liberties groups thwarted the implementation of this system; however the desire of governments to retain or require a 'backdoor' deposited with a third party (called an escrow agent) that will permit the deciphering of encrypted communications continues to be a major point of tension.

See also: **Encryption; Algorithm; Cryptography; Escrow; and Escrow agent**

For more information:

<http://www.epic.org/crypto/clipper/>

<http://www.cdt.org/crypto/clipper.html>

http://www.webopedia.com/TERM/C/Clipper_chip.html

<http://www.law.miami.edu/~froomkin/articles/clipper.htm>

Closed Circuit Television (CCTV):

A term more frequently used in the UK, CCTV is a visual surveillance technology designed for monitoring a variety of environments and activities. CCTV systems typically involve a linked system of cameras which are able to be operated remotely from a control room.

While Britain is clearly the lead nation in implementing CCTV, other countries are quickly following. North America, Australia and some European countries are installing the cameras in a variety of urban environments. Some groups which have been fighting the use of CCTVs are Privacy International in the UK and EPIC in the US.

Resources:

[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-61925&als\[theme\]=Video%20Surveillance&headline=CCTV%20Frequently%20Asked%20Questions](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61925&als[theme]=Video%20Surveillance&headline=CCTV%20Frequently%20Asked%20Questions)

<http://www.epic.org/>

Computer Assisted Passenger Pre-Screening System (CAPPS II) [Secure Flight]:

CAPPS II is a controversial program proposed by the United States Transportation Security Administration (TSA) in January of 2003 to combat terrorism and prevent hijacking of U.S. flights. CAPPS II is a passenger profiling and surveillance system that requires individuals to give personal information such as date of birth, home phone number, and home address before boarding a U.S. flight. Under the program, travel authorities can check these and other personal details against the information collected in government and commercial databases, then "tag" individuals with a color-coded score indicating the level of security risk that they appear to pose. Based on the assigned color/score, individuals could be detained, interrogated, made subject to additional searches, or prohibited from flying all together. The proposed CAPPS II system was regarded to be an expensive, ineffective and unnecessary invasion of travelers' privacy and was cancelled in July of 2004. CAPPSII has now been replaced by the more current Secure Flight program.

Resources:

<http://www.eff.org/Privacy/cappsii/>

<http://www.dhs.gov/dhspublic/display?content=1115>

Cookie :

A piece of information, unique to a computer that the browser saves and sends back to the server of a Web site when an individual revisits the site. The server tells a browser where to put the cookie on the computer hard drive when an individual initially visits a site. Cookies contain data such as log-in or registration information, online buying patterns in certain retail sites, user preferences, what site was last visited, etc. They allow a web site to record the user's comings and goings, usually without their knowledge or consent. Privacy advocates have argued that many companies' cookie tracking practices are a violation of individuals' privacy rights.

Resources:

<http://www.epic.org/privacy/internet/cookies/>

<http://www.cookiecentral.com/faq/>

<http://www.consumerprivacyguide.org/glossary/>

Copyright Management System:

See **Digital Rights Management (DRM)** systems.

Cross-Domain Scripting Attacks

A cross-domain scripting attack may occur when there is vulnerability in Microsoft Internet Explorer (IE) that allows a remote attacker to execute arbitrary code with the privileges of the user running IE, to read and manipulate data on web sites in other domains or zones, and/or to execute scripting code in arbitrary domains. This attack raises privacy concerns because it may lead to the disclosure of authentication information and user information, the execution of arbitrary code via a network, and/or the modification of user information.

Resources:

<http://packetstorm.linuxsecurity.com/0404-advisories/index4.html>

<http://www.securitytracker.com/alerts/2004/Dec/1012584.html>

<http://forum.gladiator-antivirus.com/index.php?s=a6a3366eaab55a9eaea7306b073bff50&showtopic=21419>

Customer Proprietary Network Information (CPNI):

Customer Proprietary Network Information is the data collected by telecommunications corporations about a customer's telecommunications provider. It includes the time, date, duration and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's bill. In recent years, CPNI has been under dispute with telecommunication company affiliates, competitors, and other third parties.

Resource:

<http://www.epic.org/privacy/cpni/>

Customer Relationship Management (CRM)

CRM is a term that generally refers to all aspects of interaction a company has with its customers (both sales and service related). More recently, the term refers to the use of information technology to differentiate and manage customer behavior and experience. The Electronic Privacy Information Center (EPIC) reports that current CRM practices allow companies to "collect information derived from a number of resources to build comprehensive

profiles on individuals in order to sell products and to sell dossiers on behavior [...] This is often done without notice or extending a choice to the individual to opt-out of the dossier building. These dossiers may be used by marketers for target advertising, customer profiling, and they may be made accessible to government for law enforcement purposes.”¹

Reference:

1. <http://www.epic.org/privacy/profiling/>

Other Resources:

<http://www.webopedia.com/TERM/C/CRM.html>

The Panoptic Sort: A Political Economy of Personal Information by Oscar H. Gandy, Jr. (Westview Press: 1993)

Cyberspace:

A term coined by author William Gibson in his 1984 novel Neuromancer. Initially, Gibson used the term to refer to a vast electronic matrix of data controlled by powerful corporate entities. Today, it refers to electronic “space” and communities on computer networks and the Internet.

Resource:

<http://www.mhhe.com/socscience/english/holeton/glossary.mhtml>

Data Controller:

A data controller is an individual or entity (company, government department and voluntary organization) that controls and is responsible for the processing, keeping and use of personal information under its care. Examples of data controllers include general practitioners, pharmacists and politicians who keep personal information about their patients, clients, constituents.

While all data controllers must comply with certain rules about how they collect and use personal information, some must register annually with the Data Protection Commissioner, in order to make transparent their data handling practices.

Resource:

www.informationcommissioner.gov.uk/

Data Encryption Standard (DES)

DES is the first official U.S. government cipher intended for commercial use. Data Encryption Standard originated at IBM in 1977 and was adopted by the United States National Institute of Standards and Technology (NIST). For each message that requires data encryption, DES provides 72 quadrillion or more possible encryption keys from which to choose. For it to work, both sender and receiver must use the same private key.

"DES was initially judged so difficult to break by the U.S. government it was restricted for exportation to other countries."¹ However, it is now the most widely used cryptosystem in the world and free versions of the software are widely available on bulletin board services and Web sites.

Reference:

1.

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html

Other Resources:

<http://www.rsasecurity.com/rsalabs/node.asp?id=2226>

Data Protection:

Data protection encompasses regulatory obligations regarding information collection, use, and disclosure. These schemes are predicated on a concern that improper dealings with personal data would pose a danger to privacy and individual liberties. Data protection schemes seek to protect rights and freedoms by (a) imposing obligations on the holder and/or processor of personal data and (b) conferring rights upon individuals (data subjects).

See also: **Data Subject; Fair Information Practices.**

Resources:

http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Background/2Presentation.asp - TopOfPage

http://europa.eu.int/comm./internal_market/privacy/instruments/ocdeguideline_en.htm

http://europa.eu.int/comm./internal_market/privacy/overview_en.htm

Data Quality:

Data quality refers to the fitness of data for a proposed or required use. The standard measurements of such fitness are: whether the information is complete, whether it is valid, whether it is consistent, and whether the data

is timely and accurate. Data quality is integral to meaningful data collection, warehousing and mining.

Resources:

http://en.wikipedia.org/wiki/Data_quality

http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci1007547,00.html

http://www.dataquality-research.com/topics/SDM_overview.ppt

<http://www.dataquality-research.com/>

http://www.cio.gov.bc.ca/other/daf/irm_glossary.htm - D

Data Retention:

In general, data retention concerns the amount of time that data is kept. Fair information practices require that data be retained for as short a period as possible, which is often defined as the period necessary to fulfill the purpose for which data is collected. Data retention has become a hot privacy issue in relation to proposals to require communication service providers (such as telephone companies and Internet service providers) to retain *all* traffic data of their users for a specified or indefinite period of time so that it is available to government agencies like the police and security personnel.

See also: **Fair information practices**

Resources:

http://www.epic.org/privacy/intl/data_retention.html

http://www.theregister.co.uk/2004/12/10/ec_data_retention/

<http://www.euobserver.com/?aid=17906&sid=9>

Data Subject:

A data subject is an identified or identifiable individual about whom personal information is collected, used, disclosed or processed.

In research terms, a data subject may also be a non-identified and non-identifiable participant in a research project. The data subject in this context is the subject to whom information relates even though they themselves are not knowable.

Resources:

http://europa.eu.int/comm/internal_market/privacy/instruments/ocdeguideline_en.htm

<http://www.informationcommissioner.gov.uk/eventual.aspx?pg=Glossary>

Data warehousing:

Data warehousing is a process of collecting and consolidating information from various sources into a single repository of integrated information. This implementation makes it easier and more efficient to perform queries, analysis and reporting on data that originally came from multiple sources. Privacy risks arise from data warehousing because the process facilitates data mining or outsourcing of data to "data havens" with weaker legal protections for personal information.

See also: **data mining**.

Resources:

<http://www.dwinfocenter.org/defined.html>

<http://www.datawarehousing.com/whatis.asp>

<http://www.datawarehousing.com/glossary/#D>

Digital Rights Management (DRM)

DRM is a technological system for controlling access to, and uses made of, digital content. In essence, a DRM system is a content protection system that generally comprises two elements: (1) data identifying the content and rights holders of digital content, and (2) a licensing arrangement establishing the terms of use of the work. A DRM system dictates the uses which may be made of digital content and allows for the collection and exchange of use information among rights owners and distributors. DRM systems are capable of tracking, monitoring and recording use of content by individuals. A DRM system may also employ **technological protection measures (TPM)**.

Articles 11 and 12 of the WIPO Copyright Treaty require contracting states to provide legal protection and remedies for the circumvention of TPM and against alteration of DRM. The United States' implementation of this requirement in the *Digital Millennium Copyright Act (DMCA)* has proven controversial. Proponents of the legal protection of DRM and TPM maintain that these laws are necessary to protect copyrighted works from digital piracy. Critics maintain that these laws push aside the balance struck by copyright between access and protection, skewing the equation in favour of

rights holders, and claim that the resulting imbalance correspondingly chills research and speech, imperils anonymity and privacy, undermines innovation, and opens the way for anticompetitive lawsuits that ultimately harm consumers.

Digital rights management systems are also referred to as “electronic rights management systems” (ERMS), “rights management information systems” (RMIs), “electronic copyright management systems” (ECMS) and “copyright management systems” (CMS).

Resources:

Canadian Internet Policy and Public Interest Clinic, “Digital Rights Management” (<http://www.cippic.ca/en/faqs-resources/digital-rights-management/>)

Ian Kerr, Alana Maurushat, and Christian S. Tacit, “Technical Protection Measures: Parts I and II - Trends in Technical Protection Measures and Circumvention Technologies” (http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/protection_e.pdf and http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/protection_e.pdf)

DRM Watch (<http://www.drmwatch.com/>)

Electronic Frontier Foundation, “Digital Rights Management and Copy Protection Schemes” (<http://www.eff.org/IP/DRM/>)

Berkely, The Law & Technology of DRM Conference (<http://www.law.berkeley.edu/institutes/bclt/drm/>)

“Digital Rights Management”, Wikipedia (http://en.wikipedia.org/wiki/Digital_Rights_Management)

Digital Signature:

A digital signature is a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. A digital signature serves the same purpose as a written signature, guaranteeing that the individual sending the message really is who he or she claims to be. It is a value computed from a message and the signer's private key. Since it uses the signer's private key, only the signer can generate this value. This makes it impossible for others to alter the message and generate the correct digital signature for it. The receiver of the digital signature can verify it using the signer's public key. If the digital signature cannot be verified then either the signature is fraudulent or the message has been altered.

Resources:

http://www.webopedia.com/TERM/D/digital_signature.html

<https://secure.examiner.com.au/camtech.asp>

<http://csrc.nist.gov/cryptval/dss.htm>

<http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html#Intro>

Digital Signature Algorithm (DSA):

DSA is a United States Federal Government standard for digital signatures proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS). DSA was an attempt by the Federal Government to control high security cryptography and part of that policy included prohibition of the export of high strength encryption algorithms. However, shortly after its release, DSA was discovered to be capable of encryption.

Resources:

http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

<http://www.eff.org/Privacy/Newin/dss.ps>

Digital Signature Standard (DSS):

A cryptographic standard instigated by the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard (FIPS), the Digital Signature Standard (DSS), became effective in 1994. It is now the federal standard for authenticating electronic documents, much as a written signature verifies the authenticity of a paper document. "DSS was the first cryptographic standard developed under the regime established by the Computer Security Act, which was intended to limit the role of the National Security Agency (NSA) in the development of civilian standards."¹ Private and commercial organizations were given the choice to follow the standard voluntarily without the payment of royalties to the Government.

Reference:

1. <http://www.epic.org/crypto/dss/>

Resources:

<http://csrc.nist.gov/cryptval/dss.htm>

<http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html#Intro>

<http://www.eff.org/Privacy/Newin/dss.ps>

Digitization:

Digitization is the process of converting information into a digital format. Through this process information is organized into small units of data (called bits) that can be separately addressed (usually in bit groups called bytes). Information which is converted into this format is called binary data. Computers and many devices with computing capacity process data in this format.

Resource:

http://whatis.techtarget.com/definition/0,,sid9_gci896692,00.html

Domain:

A domain is an Internet location or the Internet 'address' of a single or group of networked (linked together) computers, such as www.google.com. The location is determined by a unique address known as an Internet Protocol or IP address. The underlying address system is numeric but is converted to more readily understandable and easy to memorize words. The system used is hierarchical: at the top level (top level domain) there are major category divisions by topic (e.g. .com, .org, .net, .gov) and by country (e.g. .ca, .us, .uk). At the second or lower level is the name that identifies the particular location or computer (e.g. anonequity.org).

See also: **Internet Protocol**

Resources:

<http://computer.howstuffworks.com/dns1.htm>

<http://www.google.ca/search?hl=en&lr=&oi=defmore&q=define:domain>

<http://www.webopedia.com/TERM/d/domain.html>

Echelon:

An officially unacknowledged global spy network, led by the U.S. National Security Agency (NSA) in collaboration with the intelligence agencies of U.K., Australia, Canada and New Zealand, Echelon operates an automated system for the interception and relay of electronic communications. The organization is named after the code name for the system component responsible for intercepting satellite communications.

Echelon is perhaps the most powerful intelligence gathering organization in the world. Several credible reports suggest that this global electronic communications surveillance system presents an extreme threat to the privacy of people all over the world. It is estimated that the monitored transmissions include up to 3 billion communications daily, including all the telephone calls, e-mail messages, faxes, satellite transmissions, and Internet downloads of individuals as well as public and private organizations worldwide. The vast large amount of voice and data communications are then processed through sophisticated filtering technologies.

This massive surveillance system apparently operates with little oversight. Moreover, the agencies that are reported to run Echelon have provided few details about the legal guidelines for the project. Because of this, there is no way of knowing if the network is being used illegally to spy on private citizens. As counter-terrorist activity intensifies following the events of September 11, 2001, Echelon activity is also considered likely to intensify.

Resources:

<http://www.echelonwatch.org/>

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci560967,00.html

Electronic Data Interchange (EDI):

EDI is the transmission of business transactions from one computer to another in standard or proprietary formats. This transfer of data between different companies takes place by using networks, such as the Internet. Since most companies are now connected to the Internet, EDI has become increasingly important as an easy mechanism for companies to buy, sell, and trade information.

Roger Clarke lists the following essential elements of EDI:

- The use of an electronic transmission medium (originally a value-added network, but increasingly the open, public Internet) rather than the dispatch of physical storage media such as magnetic tapes and disks;
- The use of structured, formatted messages based on agreed standards (such that messages can be translated, interpreted and checked for compliance with an explicit set of rules);
- Relatively fast delivery of electronic documents from sender to receiver (generally implying receipt within hours, or even minutes); and
- Direct communication between applications (rather than merely between computers)¹.

Reference:

1. <http://www.anu.edu.au/people/Roger.Clarke/EC/EDIIntro.html>

Other Resources:

<http://www.aesharenet.com.au/FfE/>

Electronic Copyright Management System (ECMS):

Refer to **Digital Rights Management (DRM)** systems.

Electronic Rights Management Systems (ERMS):

Refer to **Digital Rights Management (DRM)** systems.

Extranet:

Similar to the intranet, extranet is a virtual community that links business groups through the World Wide Web. Extranet uses web technology to facilitate inter-business transactions such as placing and checking orders, tracking merchandise, and making payments between companies and organizations. Various levels of the network can be made accessible to authorized outsiders.

Resources:

<http://about-the-web.com/shtml/glossary.shtml>

<http://www.webopedia.com/TERM/e/extranet.html>

File sharing:

File sharing is the act or state of allowing multiple individuals or computers access to the same data or files on a computer or network. Shared files may be stored and made available on individuals' personal computers or through a central file server that multiple individuals can access. Shared files may be downloaded, read, copied, printed or modified by more than one individual. Access and use controls can be implemented with respect to shared files in order to prevent, for example, multiple users from modifying the same file simultaneously. In the Internet context, 'file sharing' commonly refers to the phenomenon of making shared files available – also known as 'uploading' – to other Internet users for them to download. File sharing in this context usually takes the form of "peer-to-peer" or "P2P" file sharing, whereby shared files are stored and made available on individual users' personal computers. See definition of "peer-to-peer" below. In some file sharing

applications, users are able to simultaneously download a shared file or parts of a shared file from multiple sources, thereby increasing the speed of the download.

Resources:

<http://www.angelfire.com/ny3/diGi8tech/FGlossary.html>

http://en.wikipedia.org/wiki/File_sharing

http://www.canfli.org/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=2

Filter:

A filter is commonly understood as a program or device that identifies specified terms and then directs a particular action in connection with the identified terms. The actions include: blocking access to or from Web sites, content and locations; customizing content according to selected preferences; and, directing, sorting, filing or discarding e-mail containing filtered terms.

See also: **Client based filter**

Resources:

<http://www.webopedia.com/TERM/f/filter.html>

<http://www.google.ca/search?hl=en&lr=&oi=defmore&q=define:Filters>

Firewall:

A firewall is a system used both in hardware and software to prevent unauthorized access to or from a private network. Firewalls are usually used to secure private networks connected to the Internet, and especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Network security analysts distinguish between a personal firewall which is a software application that filters the traffic flow in and out of a single computer; and a traditional firewall which usually runs on a dedicated network device or computer positioned on the boundary of two or more networks or DMZs (demilitarized zones). The latter firewall filters all traffic entering or leaving the connected networks.

There are also several types of firewall techniques which have been distinguished¹:

- Packet filters: Look at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
 - Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.
 - Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
 - Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.
- In practice, many firewalls use two or more of these techniques in concert.

Reference:

1. <http://www.pltdsl.com/support/gdisplay.asp?stub=F>

Resources:

<http://www.pcreview.co.uk/article-7388.php>

http://en.wikipedia.org/wiki/Firewall_%28networking%29

Global Positional System (GPS):

A worldwide radio-navigation system, launched by the U.S. Air Force in 1978, GPS is composed of a constellation of 24 satellites and their ground stations. The system was declared fully operational for civilian applications in December 1993. GPS uses a standardized procedure to determine positional coordinates that are accurate up to centimeter-level anywhere on the surface of the Earth.

Today, GPS receivers have been miniaturized to just a few integrated circuits and are becoming very economical thus, making the technology accessible to virtually everyone. The system is now available in cars, boats, planes, construction equipment, movie-making gear, farm machinery, and even laptop computers.

Resources:

<http://www.oceanservice.noaa.gov/topics/navops/positioning/welcome.html>

<http://www.trimble.com/gps/satellites.html>

Global System for Mobiles (GSM):

Formerly known as "Groupe Spécial Mobile" (French), GSM is a world-wide standard for digital wireless mobile phones which was first developed in 1982. The standard was originated by CEPT (European Conference of Postal and Telecommunications Administrations) and further developed by ETSI (European Telecommunications Standards Institute) as a standard for European mobile phones, with the intention of developing an open, non-proprietary standard for adoption world-wide. It has been remarkably successful, with more than one billion people using GSM phones as of early 2004. GSM is sometimes also labeled as 2G (for second generation) mobile network.

The ubiquity of the GSM standard makes intra-nation roaming very common, with international roaming frequently enabled by "roaming agreements" between operators. GSM differs from its predecessors most significantly in that both signaling and speech channels are digital.

Resources:

http://www.brainyencyclopedia.com/encyclopedia/g/gl/global_system_for_mobile_communications.html

http://en.wikipedia.org/wiki/Global_system_for_mobile_communications

Globally Unique Identifier (GUID):

A GUID is a unique 128-bit number that is produced by the some Windows applications to identify a particular component, application, file, database entry, and/or user. Every entity that needs to be uniquely identified (such as an interface) has a GUID. Likewise, every time a user account is created, a GUID is assigned to the user.

GUIDs are generated from other "unique" information on a machine and are sometimes placed in hidden fields within Microsoft documents (such as Microsoft Word), allowing the original author to be identified. Microsoft got in trouble in 1999 for automatically shipping up GUIDs as part of its registration process.

Resources:

http://linux.about.com/cs/linux101/g/GUID_Globally-.htm

<http://www.wired.com/news/technology/0,1282,18331,00.html>

<http://en.wikipedia.org/wiki/GUID>

Human Genome Project:

A genome is the entire DNA in an organism, including its genes. Genes are responsible for carrying the information that makes the proteins required by all organisms. These proteins determine, among other things, how the organism looks, functions, and sometimes even how it behaves. Begun formally in 1990 by the Department of Energy (DOE) and the National Institute for Health, the Human Genome Project was a 13 year effort with the following goals:

- *identify* all the approximately 20,000-25,000 genes in human DNA,
- *determine* the sequences of the 3 billion chemical base pairs that make up human DNA,
- *store* this information in databases,
- *improve* tools for data analysis,
- *transfer* related technologies to the private sector, and
- *address* the ethical, legal, and social issues (ELSI) that may arise from the project.¹

There has been a great deal of debate over the ethical conflicts that might develop as a result of this new technology. Some of the major concerns of DNA testing and cataloging include:

- Fairness in the use of genetic information by insurers, employers, courts, schools, adoption agencies, and the military, among others.
- Privacy and confidentiality of genetic information.
- Psychological impact and stigmatization due to an individual's genetic differences.
- Reproductive issues including adequate informed consent for complex and potentially controversial procedures, use of genetic information in reproductive decision making, and reproductive rights.
- Clinical issues including the education of doctors and other health service providers, patients, and the general public in genetic capabilities, scientific limitations, and social risks; and implementation of standards and quality-control measures in testing procedures.
- Uncertainties associated with gene tests for susceptibilities and complex conditions (e.g., heart disease) linked to multiple genes and gene-environment interactions.
- Conceptual and philosophical implications regarding human responsibility, free will vs. genetic determinism, and concepts of health and disease.
- Health and environmental issues concerning genetically modified foods (GM) and microbes.
- Commercialization of products including property rights (patents, copyrights, and trade secrets) and accessibility of data and materials.²

References:

1. http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml
2. <http://www.voidspace.org.uk/science/genome/8.shtml>

Other Resources:

<http://doegenomes.org/>

http://ny.essortment.com/humangenomepro_rcaf.htm

<http://www.er.doe.gov/production/ober/history.html>

Identity theft:

Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security, Social Insurance and/or driver's license numbers and uses it to establish credentials in the identity of another person. While some identity thieves steal and use all of one person's data for illicit purposes, others use composites of several people's information creating one single false identity, or multiple variant or fictitious identities. Recent surveys show there are currently 7-10 million victims per year in the U.S. alone. Highly vulnerable population groups include students, the elderly and the military.

Identity theft is an evolving and changing problem. While traditionally, identity theft was used for financial gains, increasingly it is being used for criminal purposes. The most common way criminals perform identity theft is through presenting other individual's data, real or counterfeit, as their own to a law enforcement officer during an investigation or upon arrest.

One of the keys to curbing identity theft lies in effective legislation designed to protect consumer rights, restricting access to personal information and assisting those who become victims of this crime to become whole again. Unfortunately, currently in most identity theft cases, the burden of clearing one's name within both financial institutions and the criminal justice system is primarily on the victim. There are no established procedures for clearing one's wrongful criminal record.

Resources:

<http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm>

<http://www.idtheftcenter.org/index.shtml>

<http://www.ftc.gov>

Instant Messaging:

Instant messaging is an online communication technology that combines email with chatting. Instant messaging notifies a user when a friend is

online, allowing for simultaneous, real-time communication. In general, both parties in the conversation see each line of text right after it is typed (line-by-line), making it more like a telephone conversation than emailing. Most services also have the ability to post the users "online status" notifying others if they are away, busy, offline, etc.

ICQ was the first general instant messenger introduced to the internet, in November 1996. After its introduction, a number of variations of instant messaging systems, each with its own protocols, have been developed. Some of the other more popular instant messaging services on the Internet include MSN Messenger, AOL Instant Messenger, and Yahoo. These services derived many of their features from an older (and still popular) online chat medium known as Internet Relay Chat (IRC). The technology is particularly popular among young pc users.

Some of the drawbacks of Instant Messaging include:

- If you aren't careful when you sign-up for the program, your account could be set up so that anyone can contact you, not just your friends.
- Most IM software encourages you to create personal profiles that may include your name, age, e-mail address, home address, phone number, school and hobbies. This information is then made available to any IM user on the Internet.
- You can receive pornographic "spam" through your instant messaging program.¹

Reference:

1.

http://www.mediaawareness.ca/english/resources/special_initiatives/wa_resources/wa_teachers/are_you_web_aware/web_aware_im.cfm

Other Resources:

http://en.wikipedia.org/wiki/Instant_messaging

Intelligent Agents [smart agents]:

Software programs/elements that work independently of a user, agents "search" the Internet according to parameters programmed into the software, and then return results directly to the home PC. Examples of such agents include: news retrieval mechanisms, shopping assistants, spam filters and game bots.

While some contend that smart agents could be employed to ensure user security and privacy since they can act as an intermediary for the user, others note with caution that intelligent agents can also be used as tools to track Web behavior: they can "watch" Web surfing to note favorite sites,

automatically download favorite sites, and even tailor specific pages to suit individual user tastes.

Resources:

http://www.webopedia.com/TERM/i/intelligent_agent.html

http://en.wikipedia.org/wiki/Intelligent_agents

http://www.cspp.org/projects/july99_cto_report.pdf

Interactive Marketing:

Interactive marketing describes buyer-seller electronic communications in a computer-mediated environment. Interactive marketing is the general term for any direct communication to a consumer or business recipient that is designed to generate a response in the form of a direct order, a request for further information that may eventually lead to a direct order, and/or a visit to a store or other place of business for purchase of a specific product(s) or service(s).

Resources:

<http://www.interactivehq.org/>

http://www.ciadvertising.org/student_account/summer_01/shasheen/finalproject/Directmarketing.html

Internet Protocols (IP):

The Internet Protocol is the method by which data is transferred from one computer to another over the Internet. These methods, or "protocols," are implemented in software and in other products used in the operation of the Internet. Data is sent in blocks referred to as packets, which are supposed to, but do not always, arrive on the other computer. The current and most popular protocol in use today is IPv4, though this is expected to be succeeded by IPv6, which can provide more addresses.

See also: **VOIP

Resources:

<http://www.webopedia.com/TERM/P/protocol.html>

<http://www.getnetwise.org/glossary>

http://en.wikipedia.org/wiki/Internet_protocol

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214031,00.html

Internet Service Provider (ISP):

An ISP is a company that sells Internet access, most often through a local phone number. ISPs are usually distinguished from commercial services, which link to the Internet but also offer additional services, such as content and chat software, only available to their subscribers.

Resources:

<http://www.consumerprivacyguide.org/glossary/>

http://en.wikipedia.org/wiki/Internet_service_provider

<http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Glossary.html>

Intranet:

Intranet is a private computer network inside a company or organization that functions like an exclusive Internet. Intranet uses web browser software to access and process the information that employees need, but the information and web pages are located on only the computers within a company. A firewall is usually used to block access from outside the Intranet.

Resources:

<http://www.matisse.net/files/glossary.html#FTP>

<http://about-the-web.com/shtml/glossary.shtml>

IP address (Internet Protocol address or number):

An IP address is a computer language that allows computer programs to communicate over the Internet. The IP address is a set of four numbers, each between zero and 255, that uniquely identifies a computer or other hardware device (such as a printer) on the Internet. It would be simple if every computer that connects to the Internet could have its own IP number, but the architects who first created the internet didn't foresee the need for an unlimited number of IP addresses. Because there are not enough IP addresses to go around, there are now two kinds.

A static IP address is a number that is assigned to a computer by an Internet service provider (ISP) to be its permanent address on the Internet. To get

around the problem of the limited number of potential static IP addresses, many Internet service providers limit the number they allocate, and economize on the remaining number of IP addresses they possess by temporarily assigning an IP address to a requesting Dynamic Host Configuration Protocol (DHCP) computer from a pool of IP addresses. The temporary IP address is called a dynamic IP address. Dynamic IP addresses last for the duration of that Internet session or for some other specified amount of time. Once the user disconnects from the Internet, their dynamic IP address goes back into the IP address pool so it can be assigned to another user.

Resources:

<http://www.consumerprivacyguide.org/glossary/>

http://en.wikipedia.org/wiki/Ip_address

Java:

Java is a network-friendly programming language, invented by Sun Microsystems, that works in conjunction with HTML to allow dynamic programs to run and interact with a computer. Java is often used to build large, complex systems that involve several different computers interacting across networks (such as transaction processing systems) but is also becoming popular for creating programs that run in small electronic devices, such as mobile telephones.

A very common use of Java is to create programs that can be safely downloaded to a computer through the Internet and immediately run without fear of viruses or other harmful agents. Using small Java programs (called "Applets") Web pages can include functions such as animations and calculators.

Resources:

<http://www.matisse.net/files/glossary.html#FTP>

<http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Glossary.html>

http://www.idea.org.uk/online_training/course/gloss.htm

Keystroke logging:

Keystroke logging is the practice of recording every key depressed on a user's keyboard. Keystroke logging can occur through software programs or

through the use of hardware devices. Keystroke logging raises privacy and human rights concerns because it can be used to spy on or monitor the keyboard activities of persons in general and particularly for purposes such as law enforcement, security or employment.

See also: **Spyware**

Resources:

http://en.wikipedia.org/wiki/Keystroke_logging

<http://www.keyghost.com/hardware-keylogger.htm>

Lawful Access:

Term used, in the Canadian context, to mean the lawful interception of communications and lawful search and seizure of information by law enforcement agencies. Lawful access rules are set out in Canada's Criminal Code, the Canadian Security Intelligence Service (CSIS) Act, the Competition Act, and other legislation. These rules generally require that police obtain a warrant or other judicial authorization in order to lawfully intercept communications, or search for and seize data. Lawful access legislation is subject to the Canadian Charter of Rights and Freedoms, which provides for the "right to be secure against unreasonable search and seizure".

The rapid evolution of technology, the increasingly wide use of Internet and wireless communications devices, and the deregulation of the communications industry have created new challenges for law enforcement agencies trying to collect evidence with respect to suspected criminal activity. In response to pressure from the law enforcement community, and in order to ratify the Council of Europe Cybercrime Convention and to meet its international commitments, the Canadian government is considering new laws that would facilitate the collection of evidence about suspected criminals by police.

Proposals include:

- requiring all service providers (wireline, wireless, and Internet) to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies;
- "data preservation orders", which could be used to require a service provider not to delete the data of an identified individual who is the subject of an investigation, for a specified period of time;
- "production orders", which could require a third party such as an ISP, to make information in its possession available to investigators within a specified time period, as set out in a court order (thus eliminating the need for a police search);

- clarifying that lawful authority for e-mail interception consists of a search warrant to seize documents or records, rather than the more onerous judicial authorization required for wiretaps (it is not currently clear which standard applies to e-mail interception under the Criminal Code); and
- establishing a national database of Customer Name and Address (CNA) information from telecommunications service providers, so as to facilitate police access to this information.

Civil society groups in Canada have expressed concern that these proposals could, if enacted, be used "to increase the means of surveillance and investigation of all citizens who use new technologies, in almost every area of their lives, even though no serious offence has necessarily been committed."¹ Critics argue that expanding lawful access in this manner would give police unnecessarily broad powers to monitor e-mail, Web surfing, instant messaging, mobile telephones and telephone services that use Internet connections, to the detriment of individual privacy and liberty.

Reference:

1. Collectif sur la surveillance électronique, Declaration on Lawful Access, Jan.22, 2003

Resources:

Dept. of Justice, Canada Lawful Access FAQ:
http://canada.justice.gc.ca/en/cons/la_al/summary/faq.html

<http://www.lexinformatica.org/cybercrime/>

Multi-State Anti Terrorism Exchange (MATRIX):

The Multi-State Anti-Terrorism Information Exchange ("MATRIX") is a state-run database system intended to allow law enforcement agencies to analyze information from multiple criminal and public record sources in near-real time, through a single web-based query. MATRIX has nothing to do with terrorism.

Since little attention was given to privacy concerns, this system came under scrutiny by privacy groups such as the [Electronic Privacy Information Center](#) (EPIC) and the [American Civil Liberties Union](#), and several of the original state partners withdrew from the MATRIX project.

See also: **Data Mining**

Resources:

<http://www.matrix-at.org/>

http://en.wikipedia.org/wiki/Multistate_Anti-Terrorism_Information_Exchange

Non-Obvious Relationship Awareness (NORA):

A technology designed to find subtle links among data. Developed by Systems Research and Development, a company that receives funding from the Central Intelligence Agency, NORA flags potential problems such as fraud, sabotage or terrorism. NORA has been deployed by U.S. government agencies such as the CIA, FBI and DHS. A companion product from the same company is called ANNA, which purports to provide privacy protection and to enhance the security of data by utilizing a trusted third party to encrypt data in such a way as to permit queries of separate data bases but requires the same third party to provide information on the source of the data upon the finding of matches.

See also: **Total Information Awareness**

Resources:

<http://www.wired.com/wired/archive/12.02/start.html?pg=4>

<http://www-306.ibm.com/software/data/db2/srdnet/nora.html>

<http://www.google.ca/search?q=cache:N9bLtO3aEQYJ:www.roguewave.com/products/sourcepro/srdc.pdf+non-obvious+relationship+awareness&hl=en>

Online profiling:

Profiling is the practice of collecting information about consumers' preferences and interests. Online profiling takes place primarily by tracking a user's online movements and actions, with the purpose of creating targeted advertisement to the resulting profiles. The practice often relies on placing cookies in the user's machine when they are using a site.

Resources:

<http://www.consumerprivacyguide.org/glossary/>

Optical Character Recognition (OCR):

OCR is a computer system designed to translate images of typewritten text (usually captured by a scanner) into machine-editable text. An OCR system enables you to take text from a book or a magazine article, scan and feed it directly into an electronic computer file, and then edit the file using a word processor.

All OCR systems include an optical scanner for reading text, and sophisticated software for analyzing images. Most OCR systems use a combination of hardware and software to recognize characters, although some inexpensive systems do it entirely through software. While extremely advanced OCR systems can read text in a variety of fonts, most still have difficulty reading handwritten text.

The potential of OCR systems is enormous because they enable users to harness the power of computers to access printed documents. The United States Postal Service has been using OCR machines to sort mail since 1965. As well, currently, OCR is being used widely in the legal profession, where searches that once required hours or days can now be accomplished in a few seconds.

Resource:

http://www.webopedia.com/TERM/o/optical_character_recognition.html

Packet Sniffer:

A packet is a unit of information carried over a computer network. Packets consist of a header (which contains the information needed to get the packet to its destination) and some type of context, such as a portion of an e-mail message.

Packet sniffers are software programs or devices that survey communications data passing over a network. The program captures each packet and decodes it. While they are a necessary tool for network management functions, they can be used maliciously to snoop or collect personal information.

Resources:

http://en.wikipedia.org/wiki/Packet_sniffer

<http://en.wikipedia.org/wiki/Packet>

<http://www.webopedia.com/TERM/s/sniffer.html>

<http://www.webopedia.com/TERM/P/packet.html>

Panopticon:

The panopticon is a concept first invented in the early 18th century by Jeremy Bentham, English civic philosopher and designer of prisons. The panopticon was a tower from which doctors, teachers, warders (authoritative figures) could spy on the behavior of patients and inmates. Each individual is always potentially seen, but never sees the others. The subjects under

surveillance never know when they are being watched, but the possibility of it is always present and so they effectively police themselves. The idea was further fleshed out by French Philosopher Michel Foucault in his book Discipline and Punish in 1975.

For Foucault, the panopticon is not just an architectural structure, but a more general model of power relations in every day life and it can be integrated into any institution (educational, medical, prisons...).

Resources:

<http://foucault.info/weblog/000026.html>

<http://cartome.org/foucault.htm>

Password:

A password is a series of characters (letters and/or numbers) that a person uses to gain and control access to a resource. It is a form of authentication that is intended to ensure that unauthorized users do not access services or others' private information. Examples include a logon for an e-mail account or a personal identification number (see PIN) at a bank machine.

See also: **Strong password, PIN**

Resources:

<http://www.webopedia.com/TERM/p/password.html>

http://www.webopedia.com/TERM/s/strong_password.html

http://searchwindowssecurity.techtarget.com/sDefinition/0,,sid45_gci914537_00.html

<http://www.securityfocus.com/columnists/245>

<http://en.wikipedia.org/wiki/Password>

P2P (Peer to Peer):

P2P is a computer network that relies on direct connections between "client" computers ("peers") for communication. In a P2P network, all computers on the network, or "nodes", are equal in that they simultaneously function as both "clients" and "servers" to other nodes on the network. Each node is able to conduct any supported interaction with any other node, despite the fact

that nodes may differ in processing capability, communications speed, and storage capacity. A P2P network may be distinguished from a client-server network, in which a dedicated computer (a "server") transmits communications to and from distributed client computers. Servers, not client computers, act as network nodes on a client-server network.

Technically, P2P networking applies to a wide variety of applications and networks that do not rely on server-client architecture. In popular parlance, P2P networking has become closely associated with file-sharing networks such as Gnutella, FastTrack, BitTorrent, and Napster. These networks offer client interfaces for relatively anonymous transfer of files between computers over the Internet. As the most commonly shared files on P2P networks include music and film, much of the content industry has concluded that these networks enable widespread copyright infringement. Content industry groups have responded with lawsuits targeting, first, the creators of the networks and client software, and later, individual users. These lawsuits have involved piercing ISP confidentiality to ascertain the identity of otherwise anonymous P2P network users. The most extreme reactions to the emergence of P2P networks include calls for outlawing the technology entirely. Proponents of P2P networks, on the other hand, describe them as powerful new technologies which should be allowed to evolve as entrepreneurs and innovators develop business models to take advantage of their features.

Resources:

Canadian Internet Policy and Public Interest Clinic, "File Sharing" (<http://www.cippic.ca/en/faqs-resources/file-sharing/>)

"Peer-to-Peer", Wikipedia (<http://en.wikipedia.org/wiki/P2P>)

Electronic Frontier Foundation, "File-Sharing: It's Music to Our Ears" (<http://www.eff.org/share/>)

Pen Register:

A pen register device is used by law enforcement to record all outgoing numbers dialed from a particular phone line. They can be installed at a telephone company, and do not require a law enforcement agent to enter a suspect's home. Pen registers are sometimes discussed in the Internet context, where data collection may include the e-mail addresses to which messages are sent by a suspect, the IP addresses used by a suspect, and the Internet URLs that a suspect visits.

See also: **Trap and Trace; Wiretapping**

Resources:

<http://www.cdt.org/security/000404amending.shtml>

<http://www.optimizemag.com/article/showArticle.jhtml?articleId=17700653&pgno=2>

Personal Autonomy (Greek: *autos*, self, and *nomos*, rule):

Personal autonomy connotes a kind of 'private space' to live and choose according to one's own reasons and motives, rather than as a product of external control or influences. It is a basic condition of moral agency, essential for holding people morally responsible for what they do. It involves a triadic relationship between a person, an intended action and a preventing condition (e.g., a fear, threat, physical constraint, social norm, or law). Personal autonomy is frequently described from two similar but distinct perspectives: (i) from an *internal perspective*, it involves one's psychological ability to make free choices; (ii) from an *external perspective*, it involves one's physical or social ability to freely act upon those choices, once made.

A loss of privacy or perhaps even the fear that one lacks control over one's own identity (whether justified or not) could diminish personal autonomy. Conversely, the ability to control the collection, use or disclosure of personal information could enhance personal autonomy. To the extent that technology can be used to diminish or enhance one's ability to avoid external control or influences, social choices about the use of technology will have a direct effect on personal autonomy. For example, the recent mass adoption of various automation technologies and sensor networks – machines that impose pre-programmed responses rather than enabling actual choice – often diminish personal autonomy. Humans operating within such systems (e.g. airport security staff or call-centre employees) often seem more like automatons than autonomous agents. However, technology can also be used to enhance personal autonomy. For example, secure electronic voting systems would allow citizens with access and know-how to exercise democratic choices without fear of reprisal.

Resources

Buss, Sarah "Personal Autonomy," *The Stanford Encyclopedia of Philosophy* (Winter 2002 Edition), Edward N. Zalta (ed.)
<http://plato.stanford.edu/archives/fall2003/entries/autonomy-moral>

MacCallum, G.C. (1967) 'Negative and Positive Freedom' *Philosophical Review* 76 (3): 312-34; repr. in D. Miller (ed.) *Liberty*, (Oxford: Oxford University Press, 1991)

"Autonomy in Ethics" *Encyclopedia of Ethics, Volume I*, Becker, Lawrence C., Becker, Charlotte B. (eds.) (London: Garland Publishing, Inc., 1992).

"Freedom and Liberty" *Routledge Encyclopedia of Philosophy, Volume 3.* ed. Edward Craig (London: Routledge, 1998)

Personal Identification Number (PIN):

A personal identification number (PIN) is a series of numbers that is used as a personal password for the purpose of permitting general access to a place or device. A PIN is commonly associated with the use of a bank or credit card to authenticate entitlement and activate functions at automatic bank machines.

See also: **Password**

Resources:

<http://www.google.ca/search?hl=en&ie=ISO-8859-1&q=define%3APersonal+identification+number+%28PIN%29&btnG=Search&meta=>

http://en.wikipedia.org/wiki/Personal_identification_number

Phishing:

Phishing is the act of sending a false email to an individual which seeks him or her to surrender private information that can be used for identity theft. Senders usually claim to be a legitimate organization or enterprise and ask that the user visit a Web site where they are to "update" information such as passwords and credit card, social security, and bank account numbers. A fake Web site is set up to steal the user's information. Because it is relatively simple to make a Web site look like a legitimate organization's site by mimicking the HTML code, phishing scams often count on people being tricked into thinking they were actually being contacted by a legitimate organization to update their account information. While phishers realize that most people will ignore their bait, some people will be caught.

Resources:

<http://www.webopedia.com/TERM/p/phishing.html>

http://www.senseient.com/bytesinbrief/bytes.asp?page=June_2004.htm

http://www.antiphishing.org/APWG_Phishing_Attack_Report-Apr2004.pdf

Ping:

Ping is a utility that tests whether an IP address or host is operating properly and thus reachable. Ping works on a sonar model, sending packets to the target and listening for replies to indicate reception.

The utility has become so ubiquitous that to "ping" is also now a verb, meaning to test whether a target is reachable and to clock the delay.

Resources:

<http://www.webopedia.com/TERM/P/PING.html>

<http://en.wikipedia.org/wiki/Ping>

Platform for Privacy Preferences (P3P):

"The Platform for Privacy Preferences (P3P) is a protocol, developed by the World Wide Web Consortium (W3C) that seeks to automate the negotiation of privacy protections between an individual and a Web site. P3P requires Internet users to reveal their privacy 'preferences' before they are allowed to access information on the Internet. P3P presumes no single privacy standard, as does the OECD Privacy Guidelines, which would provide a simple, predictable, uniform environment for online transactions. Instead, P3P proposes the development of an elaborate range of privacy 'preferences' that require individual Internet users to make selections about the collection and use of personal data, even for online activities that would not normally require the disclosure of personal information, such as simply visiting a web site."¹

Reference:

1. <http://www.epic.org/reports/pretypoorprivacy.html>

Other resources:

<http://www.w3.org/P3P/#what>

Pretexting:

Pretexting is the illegal practice of getting an individual's personal information under false pretenses. Pretexters use a variety of tactics to get personal information including fraudulent statements and impersonation. They often sell the information to people who may use it to get credit under someone else's name, steal their assets, or to investigate or sue them. Pretexting can also lead to identity theft.

Resources:

http://www.insiderreports.com/storypage.asp_O_ChanID_E_CW_A_StoryID_E_20003385

Pretty Good Privacy (PGP):

PGP is a computer program which provides cryptographic privacy and authentication.

PGP was originally designed and developed by Phil Zimmermann in 1991. He was a long-time anti-nuclear activist, and created PGP so that like-minded people could securely use BBS systems to store messages and files. Zimmermann's program required no license for non-commercial use, was free, and the complete source code was included. Shortly after it was released, PGP found its way outside the US, and in February 1993 Zimmermann became the formal target of a criminal investigation by the US Government for "munitions export without a license".

Throughout the world it is, in its various versions, the cryptosystem most frequently chosen by users. When used properly, PGP is capable of very high security and some claim that even government agencies such as NSA are incapable of directly breaking properly produced, PGP-protected messages.

While PGP can encrypt any data or files, it is most commonly used for e-mail. Plug-ins implementing PGP functionality are available for many popular e-mail applications (such as Outlook, Outlook Express, Eudora, Evolution, Mutt, Mozilla Thunderbird, Apple Mail, and many others). In contrast to security protocols like SSL, which only protect data which is on a network, PGP can also be used to protect data stored on disk, in backups, etc.

Resources:

<http://en.wikipedia.org/wiki/PGP>

<http://www.pgp.com>

<http://philzimmermann.com>

Privacy Seal:

A privacy seal is a program that certifies eligible Web sites, holding sites to baseline privacy standards. The program requires its licensees to implement certain fair information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites. Two of the more prominent privacy shield programs are sponsored by TRUSTe and the Better Business Bureau. To post these seals on a web site, a site owner must enter into a license agreement with the seal provider and agree to ongoing compliance reviews. The primary goal of privacy seals is to

offer customers an easy way to identify organizations and Web sites that follow fair information practices.

Resources:

<http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,81041,00.html>

<http://www.bbbonline.org/privacy/>

Processor Serial Number (PSN):

A PSN is the software-readable serial number originally embedded into the Intel-brand Pentium III processor chips. PSNs present privacy risks for users, because Web sites may be able to capture the identifier and use it as a persistent tracking tool. In order to address risks that Web sites might be able to access the PSN and thus compromise irrevocably the anonymity of Web users, Intel included a utility allowing the PSN to be disabled. Nevertheless, it was later shown that some Web sites could still access the PSN even when it had been disabled.

Resources:

<http://www.cdt.org/privacy/issues/pentium3/>

http://www.theregister.co.uk/2000/05/04/so_farewell_then_intel_psn/

<http://support.intel.com/support/processors/pentiumiii/sb/CS-007579.htm>

Proxy server:

A proxy server is a server that acts as an intermediary between a workstation or server and the Internet in order to protect the resources of a private network, to provide caching/filtering capabilities, and to maintain internal administrative control. It also conserves system resources by directing all outgoing and incoming data traffic through a centralized portal.

Resources:

<http://www.inetprivacy.com/a4proxy/anonymous-proxy-faq.htm>

http://www.webopedia.com/TERM/p/proxy_server.html

http://whatis.techtarget.com/definition/0,289893,sid9_gci212840,00.html

Query String:

Query string is the section of a URL that contains the search parameters when a dynamic Web site is searched. Query strings do not exist until a user puts specified terms into a database search, at which point the search engine will create the dynamic URL with a query string based on the results. Query strings typically contain '?' and '%' characters.

Resource:

http://www.webopedia.com/TERM/Q/query_string.html

Radio Frequency Identification (RFID):

RFID is an item-tagging technology that uses radio waves to automatically identify individual items. The purpose of RFID systems is to enable data to be transmitted by a portable device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag can provide information such as identification, location, or specifics about the product tagged, such as price and date of purchase. The use of RFID in tracking and access applications first appeared during the 1980s. RFID quickly gained attention because of its ability to track moving objects and is now on the verge of becoming a widespread tool. RFID tags have profound societal implications, including the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties. It may not be long before such tags are built into individual items (such as clothing), allowing an unprecedented amount of automated monitoring and surveillance of people's habits, behaviors and locations.

Resources:

<http://www.epic.org/privacy/rfid/>

<http://www.cdt.org/previousheads/dataprivacy.shtml>

<http://www.privacyrights.org/ar/RFIDHearing.htm>

Reasonable Expectation of Privacy:

The "reasonable expectation of privacy" test is the inquiry used by both Canadian and American courts to determine whether an individual has a privacy interest recognized by the Constitution. To make this determination courts employ a 'totality of circumstances' test, which has two components. First, did the individual have a subjective expectation of privacy in the circumstances and if so, second, was the expectation objectively reasonable?

That is, the individual must not only believe that she was in a private setting, but also society in general must recognize the asserted privacy interest as reasonable.

Although the determination requires a case-by-case analysis, Canadian courts have decided that there is a strong and reasonable expectation of privacy with respect to the body, in intimate places such as the home, in a biographical core of personal information or concerning information that has been provided in confidence. In non-law enforcement contexts the term has also been used to establish respective rights between parties, most notably between employer and employee, which has given employees some privacy protection against surreptitious activities such as email or phone monitoring without notice.

See also: **Privacy; Search and seizure**

Resources:

[http://www.lexum.umontreal.ca/csc-scc/cgi-bin/disp.pl/en/rec/html/2004scc067.wpd.html?query="tescling"&langue=en&selection=&database=en/jug&method=all&retour=/csc-scc/cgi-bin/srch.pl?language=en~ ~method=all~ ~database=en/jug~ ~query=tessling~ ~h](http://www.lexum.umontreal.ca/csc-scc/cgi-bin/disp.pl/en/rec/html/2004scc067.wpd.html?query=)

Remailer:

A remailer is a computer-based process that automatically redistributes electronic email often to multiple recipients. Remailers can be anonymous. For instance an anonymous remailer can be configured to take out the information identifying the sender of a message, while still enabling a return 'path' so that recipients can reply to the messages. Some remailers however, allow users to use their real name on the message.

Resource:

<http://en.wikipedia.org/wiki/Remailer>

RSA Algorithm:

RSA is a popular, highly secure asymmetric cryptographic algorithm for encrypting information using public and private keys. It is named for the initials of its creators Rivest, Shamir and Adleman.

Resource:

Policy on Electronic Authorization and Authentication, Government of Canada September 1995, at

http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tbm_142/2-2_e.asp

Search and Seizure:

Search and seizure is the use of state power (particularly the police or security forces) to search or take something from the body, premises or property for investigative or evidentiary purposes. In many jurisdictions, legal and constitutional provisions impose constraints on the use of search and seizure powers. These constraints include requiring a warrant to engage in these practices and disallowing the introduction of evidence that has been obtained through an illegal or unconstitutional search or seizure.

The right to privacy has become directly or indirectly associated with limits to the state's ability to use search and seizure powers. In Canada and the United States, constitutional provisions provide a right to be secure against unreasonable search and seizures (see section 8 of the Canadian Charter of Rights and Freedoms <http://www.efc.ca/pages/law/charter/charter.text.htm> and the Fourth Amendment of the U.S. Constitution <http://caselaw.lp.findlaw.com/data/constitution/amendment04/>). Courts in these countries have interpreted these provisions to include privacy provisions or rights, which has led to a measure of constitutional protection to the right to privacy but has also resulted in the development of 'zones' of privacy in the form of person, property and information, with the body generally considered worthy of greater protection than property or information. It should be noted that the constraints only apply if there can be said to be a 'reasonable expectation of privacy' in the particular circumstances. The Europeans take a slightly different approach by explicitly providing a right of security in private life, home and correspondence which limits state search and seizure particularly in connection with these rights (not unlike the judicially determined zones of privacy in Canada and the United States). In all cases, there is an ongoing debate as to the appropriate balance to be struck between the use of search and seizure powers and the protection of important democratic individual rights such as those of privacy and democratic values that require limits on the use of state power.

See also: **Reasonable expectation of privacy**

Resources:

http://www.icclr.law.ubc.ca/Publications/Reports/International_Standards.pdf.

<http://faculty.ncwc.edu/toconnor/405/405lect04.htm>

<http://www.lexum.umontreal.ca/csc-scc/cgi-bin/disp.pl/en/rec/html/2004scc067.wpd.html?query=%22tessling%22&langue=en&selection=&database=en/jug&method=all&retour=/csc-scc/cgi->

bin/srch.pl?language=en~method=all~database=en%2Fjug~query=tesling~x=12~y=10

Secure Socket Layer (SSL):

SSL is a high-level security protocol for protecting the privacy and confidentiality of data transmitted online. The protocol allows internet communication while avoiding eavesdropping, tampering, or message forgery. SSL is based on RSA Data Security's public-key cryptography, and is an open protocol that is the industry security standard. SSL is popular among commerce servers on the web and is recognizable by the letters HTTPS in the URL.

Resources:

<http://about-the-web.com/shtml/glossary.shtml>

Secure Electronic Transaction (SET) protocol:

SET is an e-commerce protocol devised by Visa and MasterCard. It allows credit card holders to pay for purchases while protecting their personal information such as their account details and their purchasing habits.

SET requires cardholders and merchants to register before they may engage in transactions thereby keeping card details safe from third parties, but also protecting merchants from dishonest customers and vice-versa. A cardholder registers by contacting a certificate authority, supplying security details and the public half of his proposed signature key. If the applicant's registration is approved, they receive a certificate confirming that the signature key is valid. All orders and confirmations are authenticated through bearing digital signatures.

Resources:

<http://64.233.161.104/search?q=cache:tg1lGn8jUvIJ:www.cl.cam.ac.uk/users/lcp/papers/Auth/SET-overview-2002.pdf+%22SET+protocol+%22+define&hl=en#2>

Server:

A server is a software or hardware-based system that shares resources over a network. Servers may share files, applications, or route communications. Servers routinely retain logs of user activity, which may be accessed by the server's owner, law enforcement, or by employers.

Resources:

<http://en.wikipedia.org/wiki/Server>

<http://www.webopedia.com/TERM/s/server.html>

http://www.ocdsb.edu.on.ca/Student_Res/search/gloss.htm

Single Sign-On (SSO):

SSO is an authentication process in a client/server relationship where the user, or client, can enter one name and password and have access to more than one application or resources within an enterprise. Single sign-on takes away the need for the user to enter authentication information multiple times when switching from one application to another. SSO generally requires that applications delegate authentication to a middleware identity management system.

Resource:

http://en.wikipedia.org/wiki/Single_sign_on

Spider (also referred to as “crawlers”, “knowledge-bots” or “knowbots”):

A spider is as kind of bot program that is used by search engines to roam the World Wide Web and keep the search engine database of Web pages up to date. Spiders obtain new pages, update known pages, and delete obsolete ones. They also update “home” databases based on their findings. Most large search engines have several spiders operating at any given time. However, due to the enormity the Web, it can take a spider up to six months to cover it, so the information of search engines is potentially always slightly out of date.

Resources:

<http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Glossary.html>

<http://www.webopedia.com/TERM/s/spider.html>

http://en.wikipedia.org/wiki/Web_crawler

Spybot (also referred to as Spybot-S&D):

Spybot is a freeware program for Microsoft Windows that can remove or block installation of malware, spyware and adware from a computer. Spybot scans the computer hard disk and/or RAM for unwanted software.

Spybot is used to address a variety of problems with tracking cookies, system internals, Winsock LSPs, ActiveX objects and browser hijackers. The program can also protect the user's privacy to some extent by detecting and deleting usage tracks and securely deleting unwanted files. While Spybot is not a replacement for anti-virus programs, it does detect some common trojans and keyloggers.

Resources:

<http://en.wikipedia.org/wiki/Spybot>

<http://www.safer-networking.org/en/home/index.html>

Spyware:

Spyware are technologies that aid in gathering information about individuals and organizations without their knowledge. Spyware are programs that are usually secretly installed on computers in order to gather information about the user and their habits and relay that information to other parties. While most spyware tries to get the user to view advertising and/or directs them to particular web pages, some spyware also sends information about the user to other parties. Spyware can enter a computer as a virus or as a result of installing a new program. Noted privacy software expert Steve Gibson of Gibson Research explains: "Spyware is any software (that) employs a user's Internet connection in the background (the so-called 'backchannel') without their knowledge or explicit permission. Silent background use of an Internet 'backchannel' connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed consent for such use. Any software communicating across the Internet absent of these elements is guilty of information theft and is properly and rightfully termed: Spyware."¹

Reference:

1. <http://grc.com/optout.htm>

Resources:

<http://www.computerworld.com/securitytopics/security/story/0,10801,91170p2,00.html>

<http://www.matisse.net/files/glossary.html#FTP>

Strong Password:

Strong password describes a password that is designed to be particularly difficult to detect or crack. Strong passwords should contain some combination of upper- and lower-case letters, numbers and symbols. It should be at least 6-8 characters long and should not contain common dictionary words or proper names.

See also: **password; PIN**

Resources:

http://www.webopedia.com/TERM/s/strong_password.html

http://searchwindowssecurity.techtarget.com/sDefinition/0,,sid45_gci914537_00.html

<http://www.securityfocus.com/columnists/245>

Subscription data:

Subscription data is the information that an individual provides when he or she signs up to become a member or to receive a product or service. This information usually includes one's name, physical address, email address, billing information, and telephone numbers. Subscription data may enjoy lower legal protections against disclosure to law enforcement than the actual content of communications.

Resources:

<http://www.getnetwise.org/glossary#S>

Technological Protection Measure (TPM):

TPM is a technological system for restricting dealings with associated digital content to only those authorized by the rights-holder. TPMs are often associated with **Digital Rights Management (DRM)** systems.

Articles 11 and 12 of the WIPO Copyright Treaty require contracting states to provide legal protection and remedies for the circumvention of TPM and against alteration of DRM. The United States' implementation of this requirement in the *Digital Millennium Copyright Act (DMCA)* has proven controversial. Proponents of the legal protection of DRM and TPM maintain that these laws are necessary to protect copyrighted works from digital piracy. Critics maintain that these laws push aside the balance struck by copyright between access and protection, skewing the equation in favour of rights holders, and claim that the resulting imbalance correspondingly chills research and speech, imperils anonymity and privacy, undermines

innovation, and opens the way for anticompetitive lawsuits that ultimately harm consumers.

Resources:

Canadian Internet Policy and Public Interest Clinic, "Digital Rights Management" (<http://www.cippic.ca/en/faqs-resources/digital-rights-management/>)

Ian Kerr, Alana Maurushat, and Christian S. Tacit, "Technical Protection Measures: Parts I and II - Trends in Technical Protection Measures and Circumvention Technologies" (http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/protection_e.pdf and http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/protection_e.pdf)

DRM Watch (<http://www.drmwatch.com/>)

Electronic Frontier Foundation, "Digital Rights Management and Copy Protection Schemes" (<http://www.eff.org/IP/DRM/>)

"Digital Rights Management", Wikipedia (http://en.wikipedia.org/wiki/Digital_Rights_Management)

Text Messaging:

Text messaging is the act of sending short text messages to a device such as a cell phone or pager. Text messaging is used for messages that are no longer than a few hundred characters and contain no images or graphics. The term is usually applied to messaging that takes place between two or more mobile devices.

Resources:

http://www.webopedia.com/TERM/T/text_messaging.html

<http://www.text.it/mediacentre/default.asp?intPageID=130>

Total Information Awareness:

Total Information Awareness was a program of the US Department of Defense's Defense Advanced Research Projects Agency (DARPA) that would have gathered and retained vast amounts of public and private sector personal information of Americans and others in a central location for analysis by the US government. The program came under significant public criticism, which led to greater Congressional oversight, a reduction and finally the withdrawal of funding and ultimately the scrapping of the program. It is rumored that after Congress eliminated public funding for Total

Information Awareness that the project was routed to a different agency, continued under secret funding, or passed off to the private sector.

See also: **NORA**

Resources:

<http://www.epic.org/privacy/profiling/tia/>

http://www.disinfopedia.org/wiki.phtml?title=Total_Information_Awareness

http://www.eff.org/Privacy/TIA/20031003_comments.php

Traffic Data:

A general term referring to all the data that travels on an electronic communication network. Danezis from the University of Cambridge's Computer Laboratory has found the following four general categories of traffic data:

- *Subscriber data* provide a link between communication identifiers and a physical person. Law enforcement authorities can use them as a phone book: given a network address or a phone number, the individual that owns it or the home it is connected to, along with other details that a provider might have can be retrieved.
- *Communication data* provide a trace of who has talked to whom. Usually they link together communication identifiers, along with additional information such as the time and length of the connection or its status.
- *Location data* provide information about where the two (or more) ends of a communication are physically located. This might include the GSM cell of a handset, or the base station of a wireless network connection.
- *Service or Usage data*, contain information about the use that has been made of the network. While not logging the content of communications, information about the pages accessed on a web server, or the addresses to which an email was sent, can be considered as usage data.¹

During recent years a series of national and international legislative measures have been put in place to regulate access to traffic data by law enforcement authorities. These measures require telecommunications and Internet service providers to retain the patterns of communications going through the networks they control. While the primary reason given for such measures is the investigation of serious crime or terrorist activity partly perpetuated on-line, such legislation may also allow a number of government bodies access to this information.

Reference:

1.

http://www.worldcivilsociety.org/onlinenews/docs/18.09_danezis_george_wc_sf-position.pdf

Other Resources:

http://www.epic.org/privacy/intl/data_retention.html

Transmission Control Protocol (TCP):

TCP is a protocol within the Internet Protocol Suite (IPS) that allows the transfer of information and data between two computers (or “hosts”). TCP is connection-oriented and stream-oriented, as opposed to UDP

Resources:

<http://www.rdc.com.au/Glossary5.html>

http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Trap and Trace (see also Pen Register):

Similar to Caller ID, a trap and trace device is used by law enforcement to capture the originating phone numbers of all incoming calls on a selected phone line. It can be installed at the phone company and does not require an agent to enter the suspect's house. Trap and trace devices are sometimes discussed in the Internet context, where data collection may include the e-mail addresses to which messages are received by a suspect, the IP addresses used by a suspect, and the Internet URLs that a suspect visits.

See also: **Wiretapping; Pen register**

Resources:

<http://www.cdt.org/security/000404amending.shtml>

<http://www.optimizemag.com/article/showArticle.jhtml?articleId=17700653&pgno=2>

Trojan Horse:

The trojan horse describes a software program that is disguised or hidden in a seemingly benign (or even friendly) application that, once installed, is

highly destructive to existing programs and can covertly capture secure data such as passwords and keystrokes. The term is taken from a story related in Homer's Iliad that describes the surreptitious entering and subsequent capture of Troy by Greek soldiers who hid in the belly of a large wooden horse that was ostensibly being presented to the Trojans as a peace offering.

See also: **viruses, worms, spyware**

Resources:

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html

http://www.webopedia.com/TERM/T/Trojan_horse.html

Trusted Computing:

Trusted computing is the commercial term used to describe content controls built into computers at both the hardware and software levels. The purpose of trusted computing is to stop individuals from accessing, using, or disclosing protected content. The hardware portion of trusted computing provides certain security features including (a) the power to detect unauthorized modifications to software and (b) encrypted communication, authentication and reporting between the system components.

While trusted computing enables a number of important privacy-enhancing functions, it also creates new threats to privacy and anonymity that should be considered as these technologies advance (see <http://www.epic.org/privacy/tc/>) for this statement and in-depth information).

Resources:

http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php

<http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

Universal Resource Locator (URL):

URL is the standard way to give the address of any document or resource on the Internet that is part of the World Wide Web. A URL looks like this: <http://www.epic.org/privacy/>. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. The most common way to use a URL is to enter into a Web browser program, such as Microsoft Internet Explorer or Netscape Navigator.

Resources:

<http://webopedia.com/TERM/U/URL.html>

http://www.idea.org.uk/online_training/course/gloss.htm

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) transports voice communications over Internet Protocol (IP) data networks, such as the Internet, instead of over the traditional public switched telephone network (PSTN). Internet Telephony can include any type of voice, facsimile, or voice-messaging service. The service works by converting an analog voice signal into a digital format and transferring the data as IP packets over the Internet. The IP packets are later translated back into voice data for use by traditional phone networks. VoIP can enable less expensive communications, but there is a risk that routine digitization of voice communications could lead to greater ease of government surveillance.

See also: **Internet Protocol**

Reference:

<http://www.epic.org/privacy/voip/>

Other Resources:

<http://www.webopedia.com/TERM/V/VoIP.html>

<http://en.wikipedia.org/wiki/Voip>

Web bugs (sometimes referred to as Web beacons):

Web bugs are pixel tags or clear GIFs that are usually invisible to the user, these files are used along with cookies to help track the behavior of Web site visitors. Users cannot set their browsers to decline Web bugs because unlike cookies, they are just another graphic on a Web page. Web bugs are typically used by a third party to centralize monitoring from a number of different sites. They represent a threat to users' privacy since they can record even anonymous visit through individual's IP address (whereas cookies can be detected and turned off).

Web bugs are often used by large organizations that make financial gains by tracking user behavior (such as where they go and what they view) on the Web. This information can be used to create a profile of an anonymous user which, over time can provide specified details about that user's preferences

and interests. Advertisers can use this data for target advertising. Web bugs have also been used to track copyright violations on the Web.

Resources:

<http://www.computerworld.com/securitytopics/security/story/0,10801,91170p2,00.html>

<http://www.smartcomputing.com/editorial/article.asp?article=articles%2Farchive%2Fg0804%2F11g04%2F11g04.asp>

<http://www.tla.ch/TLA/NEWS/2000sec/20000724WebBugs.htm>

WHOIS database:

WHOIS is a database, originally intended to allow network administrators to find and fix problems in order to maintain the stability of the Internet. The database now exposes domain name registrants' personally identifiable information to spammers, stalkers, criminal investigators, and copyright enforcers. WHOIS policies and practices that facilitate this kind of exposure have been extremely controversial due to their infringement on individuals' privacies.

EPIC lists the following three points as critical to understand the issues surrounding WHOIS:

- WHOIS data consists of domain name registrants' contact information (including registrant's mailing address, email address, telephone number, and fax number); administrative contact information (including mailing address, email address, telephone number, and fax number); technical contact information (including mailing address, email address, telephone number, and fax number); domain name; domain servers; and other information.
- WHOIS data is globally, publicly accessible. Anyone with Internet access, including stalkers, corrupt governments who dislike international exposure, spammers, intellectual property lawyers, law enforcement, consumers, individuals, etc., has access to WHOIS data. The important point to realize here is that WHOIS data lends itself to both good faith and bad faith uses, and that investigating fraud is only one of many uses of WHOIS data.
- Domain name registrants in the .com/.org/.net top-level domains consist of businesses; individuals; media organizations; non-profit groups; public interest organizations; political organization; religious organizations; support groups; and so on (e.g. EPIC is a domain name registrant for "epic.org"). Domain name registrants share their services, ideas, views, activities, and more by way of Web sites, email, newsgroups, and other Internet media. While some domain name registrants use the Internet to conduct fraud, other domain name registrants have legitimate reasons to

protect their identities (and so their privacy and personal information) or to register domain names anonymously. For example, different political, artistic and religious groups around the world rely on the Internet to provide information and express views while avoiding persecution. Concealing their identity is crucial in this respect.¹

Reference:

1. <http://www.epic.org/privacy/whois/>

Wiretapping:

Wiretapping occurs when an individual deliberately and without consent intercepts another person's electronic communication. Wiretaps may have as their target the sender, recipient or both parties to a communication. This term is traditionally thought of in terms of telephones but now expands to other types of communications service providers.

See also: **Pen Register; Trap and Trace**

Resources:

<http://en.wikipedia.org/wiki/Wiretapping>

<http://www.epic.org/privacy/wiretap/>

<http://www.cdt.org/publications/lawreview/1997albany.shtml>

<http://www.faqs.org/rfcs/rfc2804.html>

XML Tagging:

Extensible Markup Language (XML) is a programming language that allows for the creation of identification labels that are then attached to digital information. These labels are designed to facilitate seamless and automated exchange of data between machines. In contrast to Hypertext Markup Language (HTML) where tags merely indicate the appearance of content, XML tags indicate what content means and even what types or categories of content are included in the document.

Resources:

<http://www.webopedia.com/TERM/X/XML.html>

http://domino.research.ibm.com/comm./wwwr_thinkresearch.nsf/pages/xml199.html

http://www.autonomy.com/content/Technology/Technology_Benefits/XML.html
