Compendium of "Sensitive" Information Definitions

CENTER FOR DEMOCRACY & TECHNOLOGY

March 24, 2008

Introduction

Renewed public interest in the privacy issues related to online behavioral targeting has brought increased attention to the question of what information should be considered "sensitive" in the behavioral targeting context. To assist those who are contemplating this question, the Center for Democracy & Technology has created this compendium of definitions in consultation with its Internet Privacy Working Group (IPWG), a group dedicated to building consensus around balanced solutions to online privacy issues. Culled from a wide array of statutes, self-regulatory guidelines, and policy proposals, the definitions and language compiled here all address "sensitive" information about individuals – information that has been granted some measure of special treatment.

For each statute, policy, self-regulatory program, and proposal presented below, we have provided the context for which the document was written, the definition(s) that are relevant to the topic of sensitive information, and any other supporting definitions that may be useful. The documents from which the definitions were compiled have been organized into sections based on the approach that each document takes in determining what information is considered sensitive. We identified three general approaches:

1. **Covered Entity** – This approach provides special protections for certain information when particular parties or types of organizations (commonly known as covered entities) hold, process, or use the information. Regulations that take this approach generally make no judgments about whether data is sensitive or not when it is out of the hands of the covered entity. An example of the covered entity approach is the U.S. Health Information Portability and Accountability Act (HIPAA), which requires health care providers and insurance companies to handle health information in a prescribed way, but does not address how other parties should handle that same information.

2. **Data Subject** – Some regulations deem certain information to be sensitive when it relates to particular categories of people (commonly known as data subjects). In this case, the same information about people who are not within the specified group may not be considered sensitive. An example of the data subject approach is the U.S. Children's Online Privacy Protection Act (COPPA), which applies special protections to information about children under the age of 13.

3. **Data Flow** – This approach provides heightened protection for certain types of information regardless of whether it is actually associated with an individual or held by a particular institution. Rather, the protections flow with the

information wherever it goes. A prototypical example of the data flow approach is the EU data protection directive, which requires special treatment of certain information whenever that information is processed (with a few exceptions).

At the conclusion of these three sections there is a miscellaneous section that contains definitions of terms that may be helpful in contemplating sensitive information but which are drawn from sources that do not necessarily ascribe heightened protections to particular types of data.

Covered Entity Approaches

Consumer Rights and Protections in the Behavioral Advertising Sector
http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf
(Consumer and privacy groups' filing at November 2007 FTC Town Hall)

Context:

The consumer and privacy groups' filing urges the U.S. Federal Trade Commission (FTC) to take proactive steps to adequately protect consumers as online behavioral tracking and targeting become more ubiquitous.

Relevant definition:

Sensitive Data — Advertisers should not collect, use, disclose, or otherwise process personally identifiable information about health, financial activities, sexual behavior or sexual orientation, social security numbers, insurance numbers, or any government-issued ID numbers for targeting or marketing. (Page 6)

Supporting definitions:

Personally Identifiable Information — Personally identifiable information (PII) consists of any information that can, directly or indirectly:
(1) identify an individual, including but not limited to name, address, IP address, SSN and/or other assigned identifier, or a combination of unique or non-unique identifying elements associated with a particular individual or that can be reasonably associated with a particular individual, or
(2) permit a set of behaviors or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier. Any set of actions and behaviors of an individual, if those actions create a uniquely identified being, is considered PII because the associated behavioral record can have tracking and/or targeting consequences. (Page 6)

Non-Personally Identifiable Information — Non-Personally Identifiable information (Non-PII) is:
(1) aggregated data not associated with any individual or any individual identifier, or
(2) any individual level data that is not PII. (Page 6)

Behavioral Tracking — The practice of collecting and compiling a record of individual consumers' activities, interests, preferences, and/or communications over time. (Page 6)

Behavioral Targeting — Using behavioral tracking to serve advertisements and/or otherwise market to a consumer based on his or her behavioral record. (Page 6)

Network Advertising Initiative
http://networkadvertising.org/pdfs/NAI_principles.pdf

Context:

The Network Advertising Initiative principles were developed to guide business practices with respect to online advertising services delivered by Internet network advertisers. Network advertisers facilitate Web advertising through ad serving, hosting and ad sales services on the Web.

Relevant definition:

Sensitive Data - Network advertisers shall neither use personally identifiable information about sensitive medical or financial data, sexual behavior or sexual orientation, nor social security numbers, for OPM. (Page 3)

Supporting definitions:

Online Preference Marketing (OPM) – OPM is a process used by network advertisers whereby data is typically collected over time and across Web pages to determine or predict consumer characteristics or preferences for use in ad delivery on the Web. The OPM process can use non-personally identifiable information or a combination of personally identifiable information and non-personally identifiable information. OPM does not refer to the use of data by network advertisers for Ad Delivery and Reporting. OPM excludes the use of data provided by a Web site or advertiser directly to the network advertiser and used by that network advertiser for Internet advertising solely on behalf of such Web site or advertiser. (Page 22)

Personally Identifiable Information (PII) – PII is data used to identify, contact or locate a person, including name, address, telephone number, or E-mail address. (Page 22)

Non-Personally Identifiable Information (Non-PII) – Non-PII used for OPM by network advertisers is not linked to a particular person and is typically compiled from click stream information compiled as a browser moves among different Web sites (or a single Web site) serviced by a particular network advertiser or from information provided by third parties (so long as that information is not personally identifiable to the network advertiser). (Page 22)

DMA Guidelines for Ethical Business Practice
http://www.the-dma.org/guidelines/EthicsGuidelines.pdf

Context:

The Direct Marketing Association's Guidelines for Ethical Business Practice are intended to provide individuals and organizations involved in direct marketing in all media with generally accepted principles of conduct.

Relevant definitions:

Personal Data
Data and selection criteria that by reasonable standards may be considered sensitive and/or intimate should not be disclosed, be displayed, or provide the basis for lists made available for rental, sale or exchange when there is a reasonable expectation by the consumer that the information will be kept confidential.

Credit card numbers, checking account numbers, and debit account numbers are considered to be personal information and therefore should not be transferred, rented, sold, or exchanged when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of such personally identifying numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers.

Social Security numbers are also considered to be personal information and therefore should not be transferred, rented, sold, or exchanged for use by a third party when there is a reasonable expectation by the consumer that the information will be kept confidential. Because of the confidential nature of Social Security numbers, they should not be publicly displayed on direct marketing promotions or otherwise made public by direct marketers. Social Security numbers, however, are used by direct marketers as part of the process of extending credit to consumers or for matching or verification purposes. (Page 15)

Collection, Use, and Transfer of Health-Related Data
Health-related data constitute information related to consumers':

- Illnesses or conditions
- Treatments for those illnesses or conditions, such as prescription drugs, medical procedures, devices or supplies or
- Treatments received from doctors (or other health care providers), at hospitals, at clinics, or at other medical treatment facilities (Page 16)

HIPAA Privacy Rule
http://www.hhs.gov/ocr/AdminSimpRegText.pdf

Context:

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions that required HHS to adopt national standards for electronic health care transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

Relevant definitions:

Health information means any information, whether oral or recorded in any form or medium, that:
(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. (Page 3)

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:
(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. (Page 4)

Protected health information means individually identifiable health information:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media; transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.
(2) Protected health information excludes individually identifiable health information in:
(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv) *(student health records)*;

and
(iii) Employment records held by a covered entity in its role as employer. (Page 5)

Gramm-Leach-Bliley
http://www.ftc.gov/os/2000/05/65fr33645.pdf

Context:

The Gramm-Leach-Bliley Act required the FTC (and other federal regulatory agencies) to issue regulations as necessary to implement notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers to nonaffiliated third parties.

Relevant definitions:

(n)(1) **Nonpublic personal information** means:
(i) Personally identifiable financial information; and
(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
(2) Nonpublic personal information does not include:
(i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or
(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available. (Page 33680)

(o)(1) **Personally identifiable financial information** means any information:
(i) A consumer provides to you to obtain a financial product or service from you;
(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer. (Page 33680)
(2) Examples—
(i) Information included. Personally identifiable financial information includes:
(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;
(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
(E) Any information that a consumer provides to you or that you or your

agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet ‘‘cookie’’ (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) Information not included. Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses. (Page 33680)

(q) **You** includes each ‘‘financial institution’’ (but excludes any ‘‘other person’’) over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act. (Page 33681)

Video Privacy Protection Act
http://www4.law.cornell.edu/uscode/18/2710.html

Context:

The Video Privacy Protection Act amended the Federal criminal code to prohibit, with certain exceptions, the disclosure of video rental records containing personally identifiable information.

Relevant definition:

The term **“personally identifiable information”** includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

Supporting definition:

The term **“video tape service provider”** means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

Cable Communications Policy Act
http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000551----000-.html

Context:

The Cable Communications Policy Act amends the Communications Act of 1934 to set forth national policy for the regulation of cable television. Among other things, it requires a cable operator to notify a subscriber concerning the nature, use, and possible disclosures of personally identifiable information to be collected about the subscriber. It also prohibits an operator from disclosing such information or using the cable system to collect such information without the subscriber's consent.

Relevant definition:

The term **"personally identifiable information"** does not include any record of aggregate data which does not identify particular persons.

Supporting language:

(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.
(2) A cable operator may use the cable system to collect such information in order to—
(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or
(B) detect unauthorized reception of cable communications.

Customer Proprietary Network Information (CPNI) Rules
http://www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000222----000-.html

Context:

The CPNI rules make it the duty of every telecommunications carrier to protect the confidentiality of proprietary information of customers. They permit a carrier that receives proprietary information from another carrier or a customer for purposes of providing any telecommunications service to use such information only for such purpose. They also direct a carrier to disclose customer proprietary network information upon the customer's request.

Relevant definition:

The term "**customer proprietary network information**" means—
(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made

available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

Supporting definitions:

The term "**subscriber list information**" means any information—

(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

The term "**aggregate customer information**" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

Fair Credit Reporting Act (FCRA)
http://www.ftc.gov/os/statutes/031224fcra.pdf

Context:

The purpose of FCRA is to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information.

Relevant definition:

(i) The term **"medical information"** --

(1) means information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to -

(A) the past, present, or future physical, mental, or behavioral health or condition of an individual;

(B) the provision of health care to an individual; or

(C) the payment for the provision of health care to an individual.

(2) does not include the age or gender of a consumer, demographic information about the consumer, including a consumer's residence address or e-mail address, or any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy. (Page 15)

Fair and Accurate Credit Transactions Act (FACTA)
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf

Context:

FACTA was an amendment to FCRA which aimed to help prevent identity theft, improve resolution of consumer credit disputes, improve the accuracy of consumer credit records, and make improvements in consumer access to credit information.

Relevant definitions:

Credit Card—The term 'credit card' has the same meaning as in section 103 of the Truth in Lending Act:

> The term "credit card" means any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit.

(Page 117 Stat. 1955)

Debit Card—The term 'debit card' means any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor, or services. (Page 117 Stat. 1955)

Privacy Act
http://www.usdoj.gov/oip/privstat.htm

Context:

The Privacy Act of 1974 was designed to protect individuals from an increasingly powerful and potentially intrusive federal government. The statute was triggered by the report published by the Department of Health, Education and Welfare (HEW), which recommended a "Code of Fair Information Practices" to be followed by all federal agencies.

Relevant language:

Each agency that maintains a system of records shall-- [. . .]
(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

Data Subject Approaches

Children's Online Privacy Protection Act (COPPA)
http://www.cdt.org/legislation/105th/privacy/64fr59888.pdf
(Final Rule starts on page 59911)

Context:

COPPA required the FTC to enact rules governing the online collection of personal information from children under 13.

Relevant definitions:

Child means an individual under the age of 13. (Page 59889)

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;
(b) A home or other physical address including street name and name of a city or town;
(c) An e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address;
(d) A telephone number;
(e) A Social Security number;
(f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or
(g) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition. (Page 59912)

Americans with Disabilities Act (ADA)
http://www.ada.gov/pubs/ada.htm#Anchor-Sec-47857

Context:

The ADA prohibits discrimination against any individual with a disability in job application procedures, hiring or discharge, compensation, advancement, and training. It also prohibits discrimination against such individuals by a public entity, on public transportation, or in public accommodations, and requires telecommunications carriers to provide functionality to support hearing- and speech-impaired individuals.

Relevant definitions:

Chapter 126:

Sec. 12102.
The term "**disability**" means, with respect to an individual
(A) a physical or mental impairment that substantially limits one or more of the major life activities of such individual;
(B) a record of such an impairment; or
(C) being regarded as having such impairment.

Sec. 12111.
The term "**qualified individual with a disability**" means an individual with a disability who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires. For the purposes of this subchapter, consideration shall be given to the employer's judgment as to what functions of a job are essential, and if an employer has prepared a written description before advertising or interviewing applicants for the job, this description shall be considered evidence of the essential functions of the job.

Sec. 12112. Discrimination (a) General Rule
No covered entity shall discriminate against a qualified individual with a disability because of the disability of such individual in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment.

Code of Federal Regulations, Title 42, Chapter I, Part 2 –
Confidentiality of Alcohol and Drug Abuse Patient Records (42 CFR 2)
http://a257.g.akamaitech.net/7/257/2422/16nov20071500/edocket.access.gpo.gov/cfr_2007/octqtr/42cfr2.11.htm

Context:
The 42 CFR 2 regulations impose restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program.

Relevant definitions:

Patient identifying information means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information. The term does not include a number assigned to a patient by a program, if that number does not consist of, or contain numbers (such as a social security, or driver's license number) which could be used to identify a patient with reasonable accuracy and speed from sources external to the program.

Records means any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program.

Patient means any individual who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program and includes any individual who, after arrest on a criminal charge, is identified as an alcohol or drug abuser in order to determine that individual's eligibility to participate in a program.

Supporting definitions:

Diagnosis means any reference to an individual's alcohol or drug abuse or to a condition which is identified as having been caused by that abuse which is made for the purpose of treatment or referral for treatment.

Treatment means the management and care of a patient suffering from alcohol or drug abuse, a condition which is identified as having been caused by that abuse, or both, in order to reduce or eliminate the adverse effects upon the patient.

Alcohol abuse means the use of an alcoholic beverage which impairs the physical, mental, emotional, or social well-being of the user.

Drug abuse means the use of a psychoactive substance for other than medicinal purposes which impairs the physical, mental, emotional, or social well-being of the user.

Program means:

(a) An individual or entity (other than a general medical care facility) who holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment; or

(b) An identified unit within a general medical facility which holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment; or

(c) Medical personnel or other staff in a general medical care facility whose primary function is the provision of alcohol or drug abuse diagnosis, treatment or referral for treatment and who are identified as such providers.

Violence Against Women and Department of Justice Reauthorization Act of 2005
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h3402enr.txt.pdf

Context:

VAWA created new penalties for gender-related violence and new programs encouraging states to address domestic violence and sexual assault.

Relevant definition:

PERSONALLY IDENTIFYING INFORMATION OR PERSONAL INFORMATION.—The term 'personally identifying information' or 'personal information' means individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, including—

(A) a first and last name;
(B) a home or other physical address;
(C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number);
(D) a social security number; and
(E) any other information, including date of birth, racial or ethnic background, or religious affiliation,

that, in combination with any of subparagraphs (A) through (D), would serve to identify any individual. (Page 7)

The Attorney General, through the Director of the Office on Violence Against Women, may award grants under this subtitle to States, Indian tribes, territories, or local agencies or nonprofit, nongovernmental organizations to ensure that personally identifying information of adult, youth, and child victims of domestic violence, sexual violence, stalking, and dating violence shall not be released or disclosed to the detriment of such victimized persons. (Page 47)

Supporting definitions:

DOMESTIC VIOLENCE.—The term 'domestic violence' includes felony or misdemeanor crimes of violence committed by a current or former spouse of the victim, by a person with whom the victim shares a child in common, by a person who is cohabitating with or has cohabitated with the victim as a spouse, by a person similarly situated to a spouse of the victim under the domestic or family violence laws of the jurisdiction receiving grant monies, or by any other person against an adult or youth victim who is protected from that person's acts under the domestic or family violence laws of the jurisdiction. (Page 6)

DATING VIOLENCE.—The term 'dating violence' means violence committed by a person—

(A) who is or has been in a social relationship of a romantic or intimate nature with the victim; and

(B) where the existence of such a relationship shall be determined based on a consideration of the following factors:

(i) The length of the relationship.

(ii) The type of relationship.

(iii) The frequency of interaction between the persons involved in the relationship. (Page 6)

SEXUAL ASSAULT. —The term 'sexual assault' means any conduct prescribed by chapter 109A of title 18, United States Code, whether or not the conduct occurs in the special maritime and territorial jurisdiction of the United States or in a Federal prison and includes both assaults committed by offenders who are strangers to the victim and assaults committed by offenders who are known or related by blood or marriage to the victim. (Page 8)

STALKING.—The term '**stalking'** means engaging in a course of conduct directed at a specific person that would cause a reasonable person to—

(A) fear for his or her safety or the safety of others;

(B) suffer substantial emotional distress. (Page 8)

Data Flow Approaches

California Data Breach Notification Law

Context:

The California data breach notification law requires state government agencies, companies, and nonprofit organizations to notify California customers if personal information maintained in computerized data files has been compromised by unauthorized access.

Relevant definitions:

California Civil Code Section 1798.29:
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29

(e) For purposes of this section, **"personal information"** means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(1) Social security number.
(2) Driver's license number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(4) Medical information.
(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
(2) For purposes of this section, **"medical information"** means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
(3) For purposes of this section, **"health insurance information"** means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

California Civil Code Section 1798.80:
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

(e) **"Personal information"** means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or

description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.

EU Data Protection Directive
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Context:

The EU data protection directive was developed to harmonize data protection across the EU, remove potential obstacles to cross-border flows of personal data, and ensure a high level of data protection within the EU.

Relevant language:

Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. (Article 8)

Supporting definition:

'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

United Kingdom -- Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Context:

The UK Data Protection Act was enacted to fulfill the requirements of the EU data protection directive.

Relevant definition:

In this Act **"sensitive personal data"** means personal data consisting of information as to—

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. (Section 2)

Supporting definitions:

"data" means information which—
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 (Section 1)

"data subject" means an individual who is the subject of personal data (Section 1)

"personal data" means data which relate to a living individual who can be identified—
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Section 1)

(1) In this Act **"accessible record"** means—
(a) a health record as defined by subsection (2),
(b) an educational record as defined by Schedule 11, or
(c) an accessible public record as defined by Schedule 12.
(2) In subsection (1)(a) "health record" means any record which—
(a) consists of information relating to the physical or mental health or condition of an individual, and
(b) has been made by or on behalf of a health professional in connection with the care of that individual. (Section 68)

Spain – Organic Law 15/1999 of 13 December on the Protection of Personal Data
https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf

Context:

Spain's data protection law was enacted to fulfill the requirements of the EU data protection directive.

Relevant definition:

Files created for the sole purpose of storing personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life remain prohibited. (Article 7)

Italy – Personal Data Protection Code
http://www.garanteprivacy.it/garante/document?ID=311066

Context:

Italy's data protection law was enacted to fulfill the requirements of the EU data protection directive.

Relevant definitions:

'sensitive data' shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life

'location data' shall mean any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

Supporting definitions:

'personal data' shall mean any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number;

'traffic data' shall mean any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

'electronic communications network' shall mean transmission systems and switching or routing equipment and other resources which permit the conveyance of signals by wire,

by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, networks used for radio and television broadcasting, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, and cable television networks, irrespective of the type of information conveyed;

'electronic communications service' shall mean a service which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, to the extent that this is provided for in Article 2, letter c) of Directive 2202/21/EC of the European Parliament and of the Council of 7 March 2002

TRUSTe Web Privacy Seal Program

Context:

The TRUSTe Web Privacy Seal marks companies that adhere to TRUSTe's strict privacy principles, and comply with the TRUSTe Watchdog dispute resolution process.

Relevant definitions:

http://www.truste.org/pdf/Web_Privacy_Seal_Program_Amendment.pdf
"**Personally Identifiable Information**" means any information collected through the Site (i) that identifies or can be used to identify, contact, or locate the person to whom such information pertains or (ii) from which identification or contact information of an individual person can be derived. Personally Identifiable Information includes, but is not limited to: name, address, phone number, fax number, email address, financial profiles, medical profile, social security number, and credit card information. Additionally, to the extent unique information (which by itself is not Personally Identifiable Information) such as, but not necessarily limited to, a personal profile, unique identifier, biometric information, and/or IP address is associated with Personally Identifiable Information, then such unique information also will be considered Personally Identifiable Information. Personally Identifiable Information does not include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual. (Exhibit B, Page 1)

http://www.truste.org/docs/Web_Seal_Self_Assessment_Form.doc
"**Sensitive Information**" includes social security numbers, and financial account and transaction information, and health information, that is connected to Personally Identifiable Information. (Page 22)

Platform for Privacy Preferences (P3P) Specifications
http://www.w3.org/TR/P3P11/#Categories

Context:

The Platform for Privacy Preferences Project (P3P) enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate.

Relevant definitions:

Physical Contact Information: Information that allows an individual to be contacted or located in the physical world -- such as telephone number or address.

Online Contact Information: Information that allows an individual to be contacted or located on the Internet -- such as email. Often, this information is independent of the specific computer used to access the network. (See the category “Computer Information”)

Unique Identifiers: Non-financial identifiers, excluding government-issued identifiers, issued for purposes of consistently identifying or recognizing the individual. These include identifiers issued by a Web site or service.

Purchase Information: Information actively generated by the purchase of a product or service, including information about the method of payment.

Financial Information: Information about an individual's finances including account status and activity information such as account balance, payment or overdraft history, and information about an individual's purchase or use of financial instruments including credit or debit card information. Information about a discrete purchase by an individual, as described in "Purchase Information," alone does not come under the definition of "Financial Information."

Computer Information: Information about the computer system that the individual is using to access the network -- such as the IP number, domain name, browser type or operating system.

Navigation and Click-stream Data: Data passively generated by browsing the Web site -- such as which pages are visited, and how long users stay on each page.

Interactive Data: Data actively generated from or reflecting explicit interactions with a service provider through its site -- such as queries to a search engine, or logs of account activity.

Demographic and Socioeconomic Data: Data about an individual's characteristics --

such as gender, age, income, postal code, or geographic region.

Content: The words and expressions contained in the body of a communication -- such as the text of email, bulletin board postings, or chat room communications.

State Management Mechanisms: Mechanisms for maintaining a stateful session with a user or automatically recognizing users who have visited a particular site or accessed particular content previously -- such as HTTP cookies.

Political Information: Membership in or affiliation with groups such as religious organizations, trade unions, professional associations, political parties, etc.

Health Information: information about an individual's physical or mental health, sexual orientation, use or inquiry into health care services or products, and purchase of health care services or products.

Preference Data: Data about an individual's likes and dislikes -- such as favorite color or musical tastes.

Location Data: Information that can be used to identify an individual's current physical location and track them as their location changes -- such as GPS position data.

Government-issued Identifiers: Identifiers issued by a government for purposes of consistently identifying the individual.

Miscellaneous Definitions

49 USC 44903 (Air transportation security)
http://www.law.cornell.edu/uscode/search/display.html?terms=biometric&url=/uscode/html/uscode49/usc_sec_49_00044903----000-.html

Biometric identifier information. — The term "biometric identifier information" means the distinct physical or behavioral characteristics of an individual that are used for unique identification, or verification of the identity, of an individual. (Section 7)

Biometric identifier. — The term "biometric identifier" means a technology that enables the automated identification, or verification of the identity, of an individual based on biometric information. (Section 7)

Who Goes There? Authentication Through the Lens of Privacy
National Research Council
http://books.nap.edu/html/whogoes/appC.html

Biometrics is the automatic identification or identity verification of individuals on the basis of behavioral or physiological characteristics.