The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters for Data Protection

Joel R. Reidenberg (*)

The exponential growth and fluidity of information circulating on the Internet pose a critical challenge to the protection of privacy. Clickstream data along with distributed computing disperses personal information and obscures information practices from public view. Few users have the means or ability to track the electronic traces of their network activities, identify the collectors and processors of their personal information or obtain redress for unfair information practices at remote locations. These characteristics of the information infrastructure ironically place democratic society in a dilemma. The Net increases the ease and economic value of the mass collection of personal information.

Yet, such citizen surveillance, whether by government or powerful private organizations, impinges on the political rights of each individual citizen in a democracy. (See Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707 (1987.)) Existing data protection laws in many countries around the world strive to preserve the rights of citizens confronted by the computerization of personal information and seek to assure that those rights will be respected when personal information is exported. (See Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States, 80 Iowa L. Rev. 431 (1995). But, government regulators and agencies as well as judicial authorities face significant jurisdictional problems applying national data privacy laws as well as enforcing territorially-based obligations to the global information infrastructure and its new digital environment. (See Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Texas L. Rev. -- (forthcoming); Joel R. Reidenberg, Governing Networks and Rule Making in Cyberspace, 45 Emory L. J. 911 (1996)).

The same information infrastructure that creates the privacy dilemma may also offer opportunities to develop and implement fair information practice rules that preserve citizens' rights while further enhancing economic value. Labeling and filtering technology, in particular, can provide a means to implement fair information practices on the Internet and assure compliance with a variety of national data protection laws. The Platform for Internet Content Selection ("PICS") is a prime example of such a technology. PICS was designed to allow selective blocking of access to content on the Internet so that parents could supervise their children's browsing. The technology itself is an HTML protocol. The protocol defines a standard format for rating labels, a "vocabulary," that can be used to describe the content of a site, allows "rating labels" to be assigned based on the vocabulary, and defines a standard mechanism for distributing the labels. (See Paul Resnick & James Miller, PICS: Internet Access Controls without Censorship, Comm. of the ACM 39 (10): 87-93 (1996) also at <http://www.w3.org/PICS/iacwcv2.htm>). With this standardization, software can then be designed to filter access to web sites with assigned rating labels that do not match user viewing preferences. The protocol does not, however, establish any particular substance for the vocabulary, any description or actual rating of web site content nor any criteria for filtering access to web sites. These are left for Net participants. Anyone can write a PICS compliant vocabulary and rating labels may be assigned by web sites on a self-

reporting basis or by third parties. Similarly, these vocabularies and rating labels may be accessible on public servers or closed systems.

As a consequence of the technical design for PICS, a standard format rating label or vocabulary can be written to describe a web site's information practices rather than its content. (See Federal Trade Commission, Workshop on Consumer Privacy and the Global Information Infrastructure, June 4, 1996 (statement of Dr. Paul Resnick, AT&T Laboratories-- Public Policy Research), available at <http://www.ftc.gov>)). Sites can then be rated according to the vocabulary and the rating labels can be distributed by the same PICS mechanism originally developed for content. Just as software such as Microsoft Explorer 3.0 can filter rating labels for content, the same filters can be configured to screen sites according to their rating labels for privacy practices. More sophisticated PICS-based technology such as the "Platform for Privacy Protection" (P3) under development by the World Wide Web consortium may also allow for differentiated filtering so that web s ites and users can negotiate the treatment of personal information rather than be limited to an all or nothing decision regarding access to the site. (See Joseph Reagle, P3 Prototype Script (Version 3.0)) <http://www.w3.org/Talks/970612-ftc/ftc-mast.html>).

As a solution for data protection and for international data flows, PICS and P3 can be a valuable instrument. This technology allows for customization of information privacy between web sites and users while offering a means of automatic enforcement-- if the web sites policies are unsatisfactory for the user, the connection is blocked. However, PICS/P3 is not a magical solution. There are a number of thorny issues and difficulties in implementing this approach.

TRANSLATING PRIVACY PRINCIPLES INTO TECHNICAL LABEL SPECIFICATIONS AND RATING LABELS

The translation of privacy principles into technical label specifications and the assignment of rating labels allows the co-existance of many different privacy policies and requires a range of decisions based on data protection values. These decisions will determine whether the technical infrastructure can accurately implement any particular set of data protection principles.

Coding and Rating

For labeling and filtering technologies to be a viable means of assuring fair information practices, data protection norms and principles must be translated into technical "vocabularies." This means that principles must be coded into labels and a numeric language that a computer processor will understand. As an illustration, one of the foundations of data protection is that a purpose for the collection and use of personal information be specified by the time of data collection. (Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data, O.E.C.D. Doc. (C 58 final), art. 7 (Oct. 1, 1980); Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Eur. T.S. No. 108, art. 5(b) (Jan. 28, 1981); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data, O.J. L281/31, art. 6(1)(b) (23 Nov. 1995)). This principle can be expressed in terms of a label definition as follows:

P=Purpose

0=Specified

1=Not specified

The rating label for a web site that did in fact specify the purpose for collecting personal information no later than the time of collection would be: p 0 For a web site that did not conform to this principle the label would be: p 1

The versatility of the PICS protocol design allows the co-existance of multiple vocabularies. For example, one set of label definitions can be used to describe information practices in terms of the Canadian Standards Association model code (Canadian Standards Association, Model Code for the Protection of Personal Information CAN/CSA-Q830-1996, (March 1996)), while another can be used to describe the same practices in terms of the European Union's directive on data protection (see supra; see appendix for model vocabularies.) This flexibility can permit ratings and filters to apply different information policies without conflict.

The Relativity of Label Definitions and Ratings

Although data protection principles can be expressed as a PICS vocabulary, translating data protection norms into a "vocabulary" requires important value judgments. Complex, inter-related principles can be difficult to transpose into an operational format. For example, the Canadian Standards Association model code contains the following principle for "individual access" (see supra):

"Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."

While the section appears straight-forward, a logical parsing to create a PICS label definition must break the clause into various options. A PICS model for this particular provision could code the principle as:

(category (transmit-as "I")

(name "Individual Access")

(label (name "OK")

(description "Requestor receives information of existence, use and disclosure of requestor's personal information, requestor receives access to such information, individual can challenge accuracy and completeness, individual can have information amended as appropriate")

(value 0))

(label (name "No challenges")

(description "No challenges to accuracy and completeness")

(value 1))

(label (name "No correction")

(description "No correction of stored data")

(value 2))

(label (name "No access")

(description "No access to personal information")

(value 3)))

[(This example was written by the author for presentation by Paul Resnick of AT&T Laboratories at a workshop on privacy issues convened by the U.S. Federal Trade Commission. See Federal Trade Commission, Workshop on Consumer Privacy and the Global Information Infrastructure, June 4, 1996 (statement of Dr. Paul Resnick, AT&T Laboratories-Public Policy Research), available at at <http://www.ftc.gov>.]

The options and the heirarchy of the options in this example reflect choices rather than specific expressions dictated by the drafting of the data protection principle. As a result, the judgments that must be made to translate a data protection principle into a PICS compliant label are significant. These judgments will determine the capability of the PICS vocabulary to allow accurate implementation of the data protection principles.

Further relativity in the use of labels and filters to protect personal information derives from rating practices. Once a vocabulary is developed, web sites must be assigned a rating label based on the label definitions. The assignment of these rating labels may also involve subjective interpretations. (For a critique of this aspect of the PICS technology, see Jonathan Weinberg, Rating the Net, 19 Hastings Comm/Ent L.J. __ (forthcoming 1997), also available at <http://www.msen.com/~weinberg/rating.htm>). This significantly impacts on the ability of software filters to assure respect for the data protection principles. If the vocabulary is loyal to the principles, but the rating labels are assigned poorly, then the filters cannot accurately assure compliance with the principles.

RATING INFORMATION PRACTICES

The utility of rating labels for information practice thus depends on both the vocabulary for label names and the accuracy of the rating labels.

Acceptability of Vocabulary

Since the PICS protocol allows the co-existence of many vocabularies to describe a web site, any given set of label names may be more or less appropriate for rating fair information practices. For example, one would expect significant differences among any vocabularies developed by the Internet Privacy Working Group, a consortium of U.S. companies and trade associations including the Direct Marketing Association, that is trying to develop a privacy vocabulary and those potentially developed by advocacy groups such as Privacy International or the Electronic Privacy Information Center. In addition, the drafting of any vocabulary faces an important trade-off between generality and specificity. If label names and options are more specific, the filtering process will be more refined and useful. However, greater specificity in the vocabulary means that the assignment of rating labels will be more complex and the configuration of filter choices by users will be more complex. By contrast, if the v ocabulary is more general, it may be easier to implement, but less useful as a tool to assure compliance with data protection principles. Hence, the perspective of the vocabulary can be of vital significance.

Confidence in Accuracy of Ratings

The rating of information practices will only be useful if users can have confidence in the accuracy of rating labels. Rating labels may be assigned by web sites on a self-reported basis and be included in the header information transmitted along with a web page or they may be assigned by a third party and stored on a public accessible server, a "label host". Other variations of label transmission and storage are also possible. In the context of data protection, self-reported labels carry a low level of confidence. Unlike content labeling, users are unable to determine the accuracy of a self-reported label. If a pornographic site self-reports a label suggesting Disney-like content, the disparity will be readily apparent to any user. By contrast, if a marketing site self-reports a label suggesting excellent privacy practices, there will be no readily apparentway for a user to discover that the site is a principal trafficker in personal information. The weak confidence in the accuracy of sel f-reported labels can be improved dramatically through independent verification. If a reputable, independent third party can verify that the self-reported label accurately reflects the practices at the web site, the label will be trustworthy. This implies that the third party must conduct an audit of the information system of the web site. Similar trust enhancement for rating labels can be accomplished by completely independent third party labeling. In this scenario, an independent third party must conduct an audit of the web site's information system and assign rating labels. Under this scenario, for the rating labels to be trustworthy, the independent third-party must be reputable and responsible for its rating. Finally, the possibility remains that the web site may change its practices subsequent to any independent review or that a label may be forged. Trusted third party digital certificates may be used to assure a limited period of validity for the label as well as the integrity of the label.

"ESP"-- AN ENVIRONMENT SECURE FOR PRIVACY

The development and use of labeling and filters can assure an environment secure for privacy (an "ESP"). However, the necessary infrastructure still needs to be developed in important ways.

Infrastructure Requirements

For PICS compliant labels and filtering to be a satisfying solution to privacy protection on the Internet, there must be accepted, standard vocabularies. At the moment, the principal development efforts undertaken by W3C and the Internet Privacy Working Group do not represent a full cross-section of citizen interests. The two groups are privately funded by their organizational members and have a distinct U.S. industry emphasis. Neither independent experts nor political actors play a significant role in framing the development efforts. This means that the results are likely to have a disproportionate weight given to the U.S. industry perspective and less balance given to citizens' interests. If acceptable, balanced vocabularies are otherwise developed, wide-spread and accessible rating labels must still be available. Filtering can only function effectively when rating labels exist and can be easily and quickly located. Should few labels be available, then either Internet use will be overly restricted throu gh the filtering of access to unrated sites or filtering will be relatively meaningless if unrated sites are not blocked. Beyond the vocabulary and rating label issues, the filtering process itself risks revealing personal information about user preferences to host web sites. This particular problem can be resolved through the use of an infrastructure architecture that includes trusted gateways. A trusted gateway can act to assure the implementation of preferences before the identity of the user can become known to the host web site.

Missing Links

At present, this "Environment Secure for Privacy" has a number of missing links. Aside from the immediate lack of any balanced, accepted privacy vocabulary and ratings, the technical infrastructure itself has missing pieces. Not all browsers offer the possibility to filter PICS compliant labels. For example, Microsoft's Internet Explorer 3.0 can read PICS labels while Netscape's Navigator 3.0 cannot. In any case, the present PICS protocol does not allow for anything other than a 'take-it or leave-it' filter process. Data protection principles, however, give much greater flexibility to negotiations between individuals and those wishing to process personal information. New protocols and software like the P3 project (see supra) must be developed to accommodate these data protection values. Likewise, the actual implementation of labels and filtering is still at a stage of infancy. Since no standard vocabulary presently exists for privacy nor are sites currently rated with PICS compliant labels for privacy, filtering is not yet ready to be a robust mechanism. Finally, if filtering is to be viable, user friendly preference files must be available to citizens. In an age when most adults have trouble programming their VCR, PICS compliant filter preferences will only work with easy implementation mechanisms such as an off-the-shelf configuration. Government Action Although the PICS technology has been available for almost two years, the private sector has proceeded only tentatively with its implementation even for the original purpose of giving parents the power to block their children's access to pornography. The movement toward the development of PICS for data protection has been inspired largely by the pressure from the U.S. Federal Trade Commission. (The original adaptation of PICS for data protection was presented at Federal Trade Commission hearings in June 1996. The P3 and Internet Privacy Working Group efforts were directed at producing prototypes for the follow-up Federal Trade Commission hear ings in June 1997.) Government, thus, must play a crucial role in the the technical development of an "Environment Secure for Privacy." By promoting vocabularies through recommendations and/or approvals, governments can advance the interests of citizens in the drafting of those vocabularies and can provide credibility to vocabularies for their public acceptance. Similarly, the existence of a balanced vocabulary with a government imprimateur can encourage the labeling of sites. Without this input, industry dominated developments are likely to continue to face serious citizen skepticism. Government may also encourage efforts to develop new protocols and software to implement easy filtering and privacy negotiations between users and web sites. In addition, government may stimulate an effective, private certification process to create confidence in the accuracy of

ratings by accrediting information practice auditors. Finally, government can recommend default filter settings to establish a fair threshold level fo r information privacy just as government establishes product health and safety standards to protect consumers.

AN INTERNATIONAL SOLUTION TO THE SEARCH FOR "ADEQUATE" PRIVACY

The ability to create an 'Environment Secure for Privacy' or ESP offers a mechanism to assure international data protection as well as satisfy a variety of national and foreigh regulatory requirements. ESP applies at the level of the network rather than at the level of any territorial jurisdiction. In particular, ESP can be a useful device to satisfy the European Union's legal prohibition on the transfer of personal information to countries that do not assure "adequate" protection for fair information practices. (Directive 95/46/EC, art. 25.) An appropriate PICS vocabulary can be created to assign rating labels for "adequacy." (A model vocabulary can be found in the Appendix below.) Rating services and label hosts can be accredited to assure the accuracy of labels. Default filter rules can be used to implement the protection. For European data protection authorities to rely on labeling and filtering technologies, these agencies will face supervisory responsibilities for technical infrastru cture arrangements. Specifically, the data protection agencies will face the following roles:

1. Vocabulary

Existing supervisory authorities will have to approve or recommend particular vocabularies like 'codes of conduct' to assure that standards are defined in terms of the European Union's Directive and national law.

2. Independently Verified Rating Labels

Existing supervisory authorities will need to require that assigned rating labels be independently verified to assure accuracy. They may also need to require digital certification to assure the authenticity of the rating abels and their timeliness.

3. Accreditation of Rating Services, Auditors, and Label Hosts

Existing supervisory authorities should accredit rating services, label hosts and auditors to assure appropriate and trustworthy implementation of labeling.

4. Non-waivable filter configurations

Existing supervisory authorities will have to define any non-waivable filter configurations to guarantee the required, minimum data protection standards. These non-waivable configurations are likely to require implementation at the server level to provide automatic and non-circumventable enforcement.

Filter Options

Existing supervisory authorities should insist that filter options be available at any infrastructure level for user choice when consent is permissible to guarantee autonomy and control of personal information by users

Trusted Gateways

Existing supervisory authorities may have to require the use of trusted gateways to assure respect for data protection during any negotiation protocol between users and collectors of personal information over the treatment of the personal information. As an international solution to the "adequacy" question posed by the European Union, there remain a number of important obstacles to the efficacy of labeling and filtering. Perhaps the most significant problem is the need and concommitant capability to rate a critical mass of web sites. Without such ratings, effective filtering cannot function. However, at the same time, the use of technologies to satisfy data protection requirements can create and stimulate entirely new service industries in the fields of information auditing, digital certification, and label hosting. These type of industries will play a critical role across the information economy in the 21st Century whether or not the impetus for their creation is data protection.

 This paper is an adaptation of presentations made to the International Working Group on Data Protection in Telecommunications (Paris, France: April 3, 1997) and to the Privacy Laws & Business 10th Annual Conference (St. John's College, Cambridge, UK: July 2, 1997).

APPENDIX

The following is an example of a PICS vocabulary that can be used to describe information practices in terms of "adequacy" for purposes of Article 25 of the EU Directive:

((PICS-version 1.0)

(rating-system "http://home.sprynet.com/sprynet/reidenberg/rating-system/")
(rating-service "http://www.rate.org/ratingsv01.html")

(name "EU Adequacy")

(description "A rating service for adequate privacy based on the EU Directive prepared by professor Joel R. Reidenberg.")

(category (transmit-as "P")

(name "Purpose Limitation")

(label (name "Specific Purpose only")

(description "Data is processed for specific purpose only, subsequent use or disclosure is not incompatible, only exemptions comply with EU Directive Article 13.")

(value 0))

(label (name "Specific Purpose most of the time")

(description "Data processed for specific purpose, subsequent use or disclosure is not incompatible, occasional exemptions.")

(value 1))

(label (name "Broad Purposes")

(description "Data processed for specific purpose, subsequent use or disclosure not always compatible.")

(value 2))

(label (name "No Limitations")

(description "Data processed without identification of specific purposes.")

(value 3)))

(category (transmit-as "Q")

(name "Data Quality")

(label (name "Accurate and Proportional")

(description "Data is accurate and up-to-date and adequate, relevant and not excessive for purposes of processing.")

(value 0))

(label (name "Usually Accurate and Proportional")

(description "Data is usually accurate and up-to-date and usually relevant and not excessive for purposes of processing.")

(value 1))

(label (name "Inaccurate or Disproportional")

(description "Data is inaccurate or is not relevant or excessive for the

purposes of processing.")

(value 2)))

(category (transmit-as "T")

(name "Transparency") (label (name "Full information provided to

individuals")

(description "Complete information provided as to purpose of processing, identity of foreign data controller, and anything else necessary to assure fairness subject only to exemptions permitted by EU Directive Articles 11(2) and 13.")

(value 0))

(label (name "Partial information provided to individuals")

(description "Some information provided as to purpose of processing, identity of foreign data controller, and anything else necessary to assure fairness subject only to exemptions permitted by EU Directive Articles 11(2) and 13.")

(value 1))

(label (name "No information provided")

(description "No information is provided regarding processing and no exemptions apply.")

(value 2)))

(category (transmit-as "S")

(name "Security")

(label (name "Security assured")

(description "Technical and organizational security measures appropriate to risks are taken by data controller.")

(value 0))

(label (name "No security") (description "Technical and organizational security measures appropriate to risks are not taken by data controller or agents of controller process data without instructions from controller")

(value 1)))

(category (transmit-as "O")

(name "Access, Rectification, Opposition")

(label (name "Data subject has full control")

(description "Data subject has access personal information, right to correct inaccurate information, right to object to processing in certain circumstances and only exemptions comply with EU Directive Article 13.")

(value 0))

(label (name "Data subject has limited control")

(description "Data subject has limited access to personal information or limited right to correct inaccurate information or limited right to object to processing in certain circumstances.")

(value 1))

(label (name "Data subject has no control")

(description "Data subject has no access personal information or no right to correct inaccurate information or no right to object to processing in certain circumstances.")

(value 2)))

(category (transmit-as "F")

(name "Further transfers to third countries")

(label (name "Adequacy assured")

(description "Further transfers to third countries permitted only where onward destination provides an adequate level of protection or authorization permitted under EU Directive Article 26.")

(value 0))

(label (name "Adequacy not assured")

(description "Further transfers to third countries permitted where onward destination may not provide an adequate level of protection without authorization under EU Directive Article 26.")

(value 1)))

(category (transmit-as "X")

(name "Sensitive Data")

(label (name "Special safeguards")

(description "Sensitive data listed in EU Directive Article 8 have additional safeguards, such as explict opt-in consent.")

(value 0))

(label (name "No special safeguards")

(description "Consumer has no ability to limit disclosure of data")

(value 1)))

(category (transmit-as "M")

(name "Direct Marketing")

(label (name "Opt-out")

(description "Opt-out available for direct marketing available at any stage.")

(value 0))

(label (name "Limited opt-out")

(description "Opt-out not always available for direct marketing.")

(value 1)) (label (name "No opt-out")

(description "Opt-out not availabe for direct marketing.")

(value 2)))

(category (transmit-as "D")

(name "Automated Decisions")

(label (name "Awareness of decision-making process")

(description "Individuals can learn the logic involved in any automated decision and measures taken to safeguard individual's legitimate interests.")

(value 0))

(label (name "No awareness of decision-making process")

(description "Individuals cannot learn the logic involved in any automated decision and measures not taken to safeguard individual's legitimate interests.")

(value 1)))

(category (transmit-as "C")

(name "Level of Compliance")

(label (name "Good")

(description "High degree of awareness among data controllers of obligations, among data subjects of their rights, existence of means of exercising rights, existance of effective and dissuasive sanctions and systems of direct verification.")

(value 0))

(label (name "Fair")

(description "Some degree of awareness among data controllers of obligations, among data subjects of their rights, existence of means of exercising rights, existance of effective and dissuasive sanctions and systems of direct verification.")

(value 1))

(label (name "Poor")

(description "Limited or no degree of awareness among data controllers of obligations or among data subjects of their rights or limited or no means of exercising rights or limited or no effective and dissuasive sanctions or system of direct verification.")

(value 2)))

(category (transmit-as "H")

(name "Support and help to data subjects")

(label (name "Available")

(description "Individual has abilility to enforce data protection rights rapidly, effectively and without prohibitive cost with some institutional mechanism to investigate independently complaints.")

(value 0))

(label (name "Unavailable")

(description "Individual does not have abilitity to enforce data protection rights rapidly, effectively and without prohibitive cost or no institutional mechanism exists to investigate independently complaints.")

(value 1)))

(category (transmit-as "R")

(name "Redress")

(label (name "Available")

(description "Appropriate redress for individual that involves compensation and sanctions through independent arbitration is available for infractions")

(value 0))

(label (name "Partially available")

(description "Redress for individuals that involves compensation or sanctions without independent arbitration is available for infractions.")

(value 1))

(label (name "Unavailable")

(description "Redress is unavailable.")

(value 2))))

* *

The following is a model PICS vocabulary based on the Canadian Standards Association privacy standard:

((PICS-version 1.0) (rating-system "http://www.privacy.org/CSA/Description/") (rating-service "http://www.privacy.org/CSA/ratingsv01.html") (name "CSA")

(description "A rating service based on the Canadian Standards Association Code for the Protection of Personal Information")

(category (transmit-as "A")

(name "Accountability")

(label (name "OK")

(description "Organization is responsible for information, designated person to assure compliance.")

(value 0))

(label (name "No designated person")

(description "No person is designated to assure compliance.")

(value 1))

(label (name "No responsibility")

(description "Organization does not take responsibility for information it collects.") (value 2)))

(category (transmit-as "P")

(name "Purpose")

(label (name "Specified")

(description "Purpose specified at or before time of collection")

(value 0))

(label (name "Not specified")

(description "Purpose not specified at or before time of collection")

(value 1)))

(category (transmit-as "C")

(name "Consent")

(label (name "Knowledge and consent")

(description "Knowledge and consent for data practices, unless inappropriate")

(value 0))

(label (name "No consent")

(description "User is told about data practices but consent may not be obtained")

(value 1))

(label (name "No knowwledge")

(description "User may not be told about data practices")

(value 2)))

(category (transmit-as "L")

(name "Limiting Collection")

(label (name "OK")

(description "Only data necessary for specified purpose, collected fairly and lawfully")

(value 0))

(label (name "Unnecessary data")

(description "Unecessary data may be collected")

(value 1))

(label (name "Unfairly collected data")

(description "Data may be collected unfairly")

(value 2))

(label (name "Unlawfully collected data")

(description "Data may be collected unlawfully")

(value 3)))

(category (transmit-as "U")

(name "Limiting Use, Disclosure and Retention")

(label (name "OK")

(description "Incompatible uses or disclosures only with consent or by the authority of law, retention no longer than necessary to fulfill purposes")

(value 0))

(label (name "longer retention")

(description "Data may be retained longer than that necessary to fulfill purposes")

(value 1))

(label (name "use or disclosure")

(description "incompatible uses or disclosures without consent, without force of law")

(value 2)))

(category (transmit-as "Q")

(name "Accuracy")

(label (name "Accurate")

(description "Accurate, complete and up-to-date for specified purposes")

(value 0))

(label (name "old")

(description "Data may be out-of-date")

(value 1))

(label (name "incomplete")

(description "Data may be incomplete")

(value 2))

(label (name "inaccurate")

(description "Data may be inaaccurate")(value 3)))

(category (transmit-as "S")

(name "Safeguards")

(label (name "Secure")

(description "Security safeguards appropriate to sensitivity of information")

(value 0))

(label (name "Insufficient safeguards")

(description "Insufficient or inappropriate safeguards")

(value 1))

(label (name "No safeguards")

(description "No safeguards")

(value 2)))

(category (transmit-as "Op")

(name "Openness")

(label (name "Open")

(description "Organization makes specific information about policies and practices available") (value 0))

(label (name "Non-specific")

(description "Organization makes non-specific information available")

(value 1))

(label (name "No information")

(description "Organization makes no information available")

(value 2)))

(category (transmit-as "I")

(name "Individual Access")

(label (name "OK")

(description "Requestor receives information of existence, use and disclosure of requestor's personal information, requestor receives access to such information, individual can challenge accuracy and completeness, individual can have information amended as appropriate")

(value 0))

(label (name "No challenges")

(description "No challenges to accuracy and completeness")

(value 1))

(label (name "No correction")

(description "No correction of stored data")

(value 2))

(label (name "No access")

(description "No access to personal information")

(value 3)))

(category (transmit-as "E")

(name "Challenging Compliance")

(label (name "Can challenge")

(description "Individual can challenge compliance to designated organizational representative")

(value 0))

(label (name "Can't challenge")

(description "No mechanism for challenge")

(value 1))))

Lex Electronica Volume 3, numéro 2 (hiver 1997)

(*) Professeur invité, Université de Paris I (Panthéon Sorbonne) 1996/97

Professor, Fordham University School of Law (New York)

E-mail: reidenberg@spynet.com
Home page: http://home.sprynet.com/sprynet/reidenberg

 ISSN 1480-1787
