ISO/IEC JTC1 SC36
Information Technology for Learning, Education, and Training

Title:

Privacy Protection and the Internet: Need for an IT-Neutral Approach

Source:

Project Co-editors

Project:

29187-1 Information technology-Identification of privacy Protection requirement pertaining to Learning, Education, and Training (ITLET) – Part 1: Framework

Document type:

Notes for Public lecture as part of the AFNOR Workshop “ITLET and Privacy Protection Standards Development” ISCC, Paris, 2010-06-30

Status:

FYI

Date:

2010-06-30

Action ID:

FYI

Distribution:

P, O, & L SC36-WG3 Members

"Privacy Protection and the "Internet" – Need for an IT-Neutral Approach"

Notes for Public lecture as part of the
AFNOR Workshop "ITLET and Privacy Protection Standards Development"
ISCC, Paris, 2010-06-30
by
Dr. Jake V. Th. Knoppers, Canada (mpereira@istar.ca)
(with the assistance of Dr. Renaud Fabre (RFabre@ccomptes.fr) Project Co-Editor
acknowledging his valuable critiques and contributions 28-29 June, 2010 on the initial draft)

Outline **Paris - 3**

Notes:

1. *The definitions and terms used in this document are based on existing ISO standards. For most of them English and French language equivalents exist.*

2. *The ISO standards referenced are all "freely available standards" and can be downloaded from ISO at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html*

3. *Dr. Renaud Fabre (France) is the ISO Project Co-Editor for the development of the new ISO standard ISO/IEC 29187 "Information technology – Identification of privacy protection requirements pertaining to Learning, Education and training (LET)".*

4. *This standard is being developed by ISO/IEC JTC1/SC36/WG3. The rationale and business case for this standards project is found in document ISO/IEC JTC1/SC36 N1737.*

5. *Since the focus of this ISCC lecture is that of privacy protection in a LET context and is based on existing ISO standards and standards development work, there will be a handout listing all ISO documents referenced as well as those of JTC1/SC36 ITLET noted in this document.(This is Annex A in this document.)*

0. Preface[1] - Shakespeare & Business Scenario Modeling

Learning, education and training are activities which require participants as interacting role players in a scenario having a common goal. Today we call this “business transaction modelling”. Whether these are business transactions modeling techniques are applied as e-commerce transactions, e-government transactions, , financial transactions, and now as “learning transactions”, the basic constructs are the same and even though there actual instantiations may all vary. There are rules, role qualifications for the players, etc. And all the participants always share a common goal, follow a basic agreed upon common script, choreography, sequencing dependencies, process and the exchange of semantic components, etc.

In this sense, perhaps the first business transaction modeller was Shakespeare as is evident by the following text,

"All the world's a stage,
and all the men and women merely players;
They have their exits and their entrances;
And one man in his time plays many parts...
Full of wise saws and modern instances..."
[Shakespeare, As You Like It, Act 2, Scene 7].

Considering all the concepts/ideas attributed to Shakespeare, one could use the above quotation to position the Bard as a prophet for EDI.

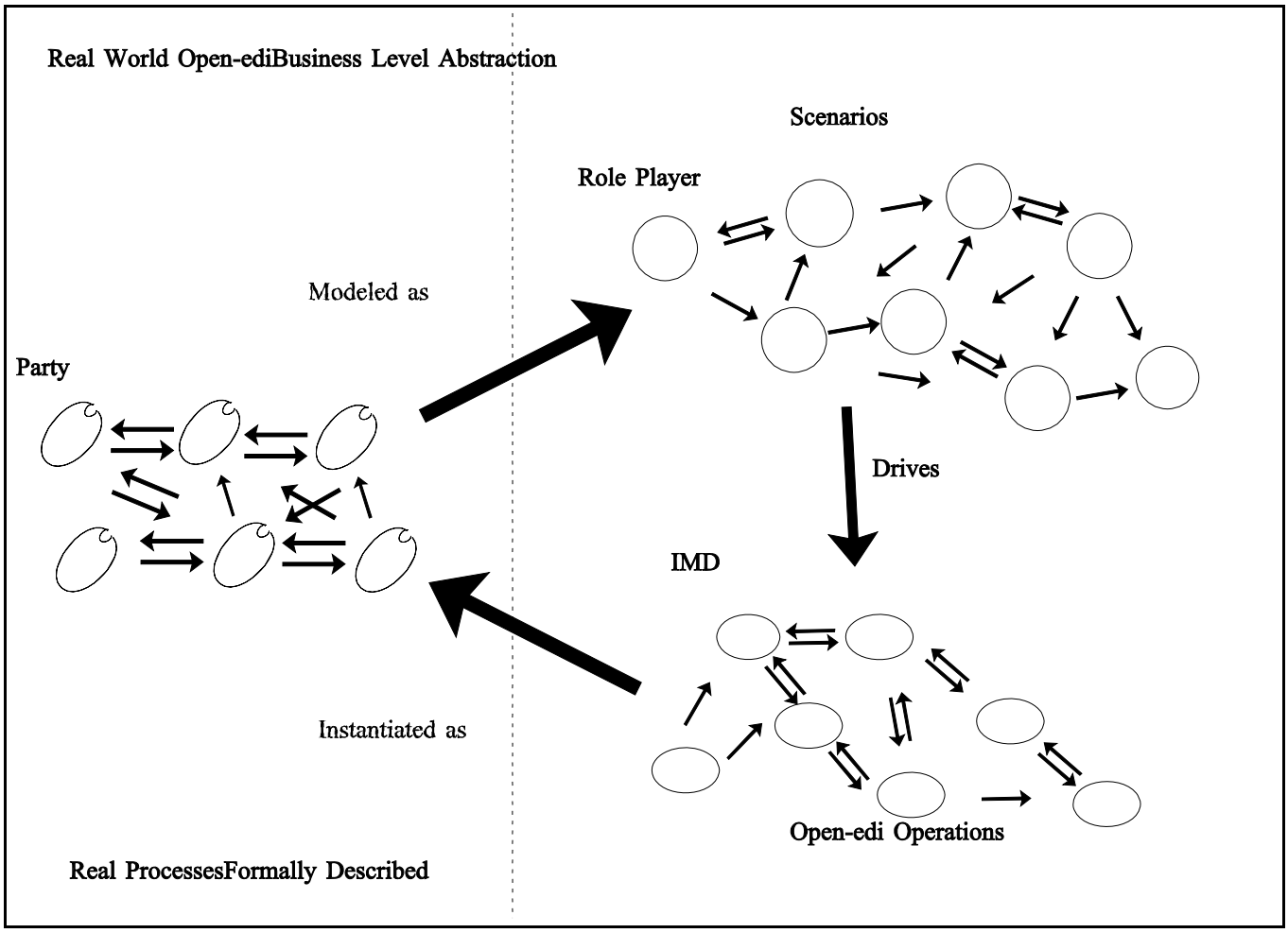
When work started in the early 1990’s on what became the 1st edition of ISO/IEC 14662 “Open-edi reference model”, one of the first questions raised was that to “What is EDI”?.

In these early deliberations on "What is EDI?", irrespective of the forum or context of the discussion, one increasingly finds the analogy of the "theatre" being used (hopefully not that of the absurd). Whether in industry sectors, standards bodies, academia, etc., concepts and terms such as scenarios, parties, agents, roles, scenes, players, etc. are increasingly being used.

The following diagram taken from the “Open-edi Conceptual Model” which preceded the “Open-edi Reference Model” standard may help provide a useful background to the today’s discussion. One needs a structured and systematic approach.

[1] Part of this text and the diagram in the Preface is taken from the articles by Dr. Jake V. Knoppers titled “*Transforming Inter-Enterprise Practices Into Open-Edi: The Business Case For Scenario Modelling*
EDI Europe Vol. 2. No. 1, 1992 by Éditions HERMES

N
Figure 2 Modelling Open-edi Transactions



1. What are the common eleven (11) principles governing privacy protection? [2] (based on OECD Guidelines, EU Directives, and APEC Framework)?[3]

Although legislation and regulations of a privacy/data protection nature differ among the many jurisdictional domains where they exist, on the whole, there are many common elements. A high level review and analysis of privacy/data protection legislation in Australia, Canada, Japan, USA, (and APEC member states), the EU, and Norway as well as Europe (both at the EU level, and that of component countries (and within country such as those of länder within Germany), etc., indicates that all these laws and regulations have common primitive requirements. These are captured and integrated below into a single set of common privacy protection principles.

The essential aspects of each of these eleven (11) common privacy protection principles and their requirements are captured below in the form of rules[4]. It is noted that for organizations and public administrations to be able to comply with these rules as external constraints which apply to them, they have to ensure that their surrounding and overarching business processes and systems may be required to be changed to be able to support external constraints of this nature.

The three most common and international recognized and accepted sources for privacy protection requirements are:

- the *1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data / Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*
  http://www.oecd.org/document/53/0,3343,fr_2649_34255_15591797_1_1_1_1,00.html

- the *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 / Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[5]
  http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

---

[2] *This is a summary presentation only. A document containing more detailed text including applicable rules and guidelines is found in document ISO/IEC JTC1/SC36/WG3 N306. This document being updated and reworked by placing it in an LET environment. The updated version will be re-issued as a new JTC1/SC36/WG3 document including more extensile text and especially the rules and guidelines associated with each Principle.*
LET = Learning, Education and Training / Apprentissage, éducation et formation

[3] One result of the work of the ISO/IEC JTC1/SC36 Ad-Hoc on Privacy was the identification an initial set of 10 Privacy Protection principles. (see document JTC1/SC36 N1436). The 11th Principle , i.e. "do no harm" , now Principle 1, was added as a result of integration with the APEC Privacy Framework,

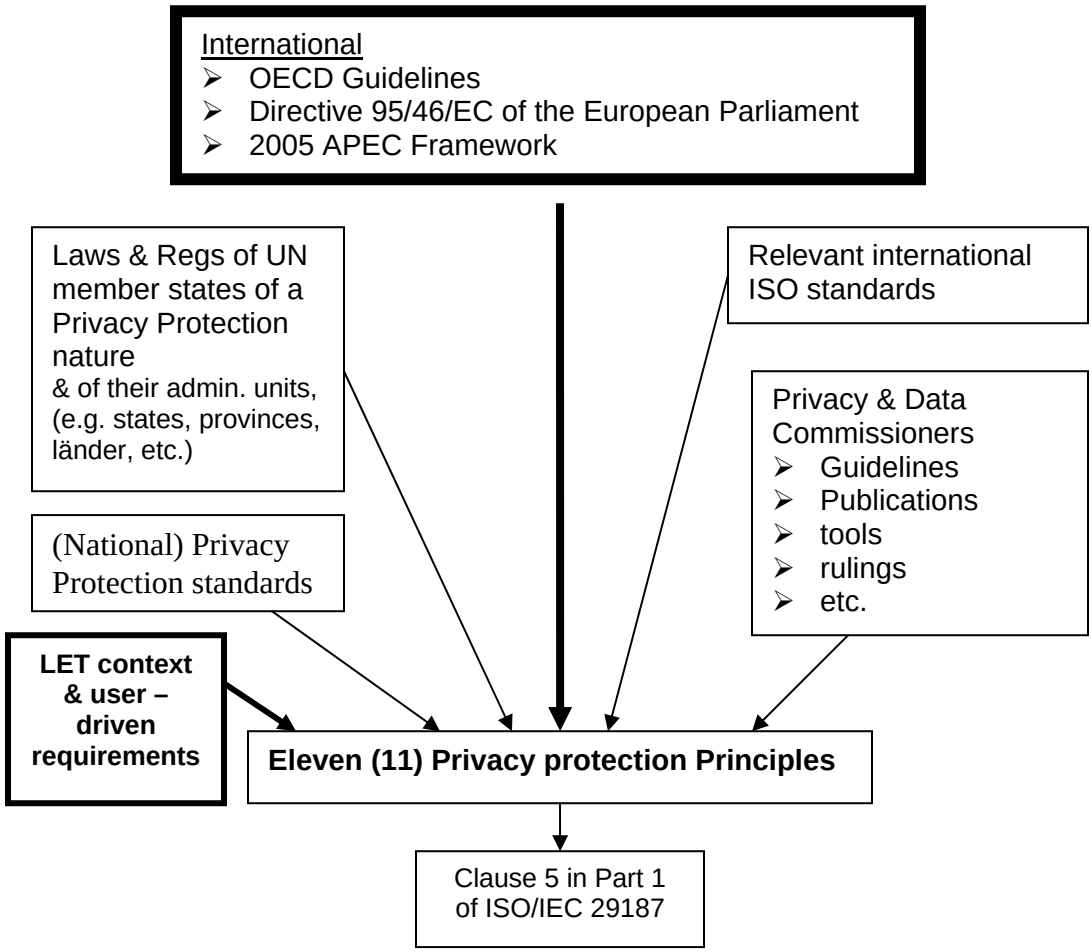
[4] The development of the Part 1 of the multipart ISO/IEC 29187 set of privacy protection and LET standard standards focuses on common primitives which are captured in the form of principles and their rules along with clearly defined concepts, i.e., as a rule-based approach in support of the Learning Operational View.

[5] This 1995 Directive is supplemented by the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) / Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques directive vie privée et communications électroniques)

- the 2005 APEC Privacy Framework
  http://www.apec.org/apec/news___media/fact_sheets/200908fs_privacyframework.html

The approach to the development of the 11 principles governing privacy protection requirements is illustrated in the following Figure A.

Figure A: Primary Sources for Privacy Protection Principles



a

In the text which follows, these eleven (11) Privacy Protection principles are placed in a LET and learning transaction context, i.e. that of the parties making a commitment on a commonly agreed upon goal for a learning transaction.

1. Privacy Protection Principle 1: Preventing Harm / "Prévention des troubles et dommages lies aux usages »

A primary objective of the preventing harm principle is to prevent misuse of personal information, and consequently harm to individuals[6]. Therefore, the implementation of privacy protection, including self-regulatory efforts, education, and awareness campaigns, as well as enforcement mechanisms, etc., should be a priority governance principle of any organization

2. Privacy Protection Principle 2: Accountability / "Accountability"

Any organization to which privacy protection requirements apply shall have in place policies and practices which make clear as to who and where, in their business operations is responsible for compliance with these external constraints as applicable to the conduct of learning transactions where the "buyer" is an "individual learner"**.** They shall so in and in an enforceable and auditable manner

An organization[7] is responsible for all personal information under its control and shall designate an organization Person, i.e. a privacy protection officer (PPO), who is accountable for the organization's compliance with established privacy principles which in turn are compliant with and support legal requirements of a privacy protection nature of the applicable jurisdictional domain(s) in which the organization operates.

3. Privacy Protection Principle 3: Identifying Purposes / "Objectifs Attendus"

The specified purpose(s) for which personal information is collected with respect to the (the (potential) goal of the learning transaction shall be identified by the organization at or before the personal information is collected.

Here the specified purpose is deemed to be the goal of the learning transaction, i.e., that mutually agreed to by the individual learner and the LET provider (at the end of the negotiation phase (and prior to the actualization) phase of the learning transaction.

4. Privacy Protection Principle 4: Informed Consent / "Consentement libre"

The principle of "informed consent" requires that the individual learner[8], be fully and explicitly informed by the Let provider as to why and for what purpose, the individual is requested (or required) to provide (additional) personal information (of various kinds), i.e., in addition to that which may be required with respect to payment aspects.

This principle is clearly a requirement for organizations to ensure that in their records keeping and IT systems to ensure that any and all personal information is "flagged" as being for limited use.

---

[6] This privacy protection principle is introduced in the APEC Privacy Framework. It can be considered an application of the generic aspect of the human rights of "do no harm", already a well and long established principle in the field of medicine.

[7] The use of the term "organization" in these Privacy Protection Principles includes "public administration".

[8] Where the individual learner is under the "age of majority", the informed consent would be provided by the parents or guardian.

5. Privacy Protection Principle 5: Limiting Collection / *"Collecte limitée"*

The collection of personal information shall be limited to only that which is necessary and relevant for the identified and specified purpose, i.e., the goal, of the specified learning transaction.

Only personal information on the individual, as an individual learner, that is essential shall be collected, i.e., that which can be proved to be relevant, for the completion of the learning transaction "in hand". This also means that any personal information that is not essential to the learning transaction shall be clearly identified, and the learning transaction shall not fail if information that is not fundamental to the learning transaction is missing.

6. Privacy Protection Principle 6: Limiting Use, Disclosure and Retention / *"Utilization, detention et présentation limitées* »

This 6th Privacy Protection Principle consolidates and integrates what are considered "generic, primitive" Information Life Cycle Management (ICLM) principles which apply to any and all types of sets of recorded information (SRIs) within an organization (including public administrations) and among organizations. This is addressed in the "collaboration space" among all parties

Personal information shall not be used or disclosed by the LET provider (or regulator) for purposes other than those for which it was collected, i.e., as part of the goal of the learning transaction, except with the informed consent of the individual, or as required by law. Secondary or derivative uses of personal information are not permitted.

Where the organization, having collected personal information for a specific purpose and goal of the execution of the learning transaction, desires to use the relevant personal information for another purpose, it is necessary to obtain revised/new "informed consent" directly from the individual concerned.

Personal information shall be retained by the LET provider only for as long as is necessary for the fulfillment of those purposes as specified as part of the learning transaction.

Personal information must be identified as having a specific 'life' of time of existence if this is to be other than that demanded for the purposes of national record keeping requirements. This retention time period for any and all personal information shall be explicitly stated.

This also means that organizations shall have in place auditable rules and procedures as are necessary to ensure that personal information no longer required for the post-actualization phase of a learning transaction shall be destroyed (expunged) by the organization, or its agents, where applicable, and in a manner which can be verified via audit procedures.

7. Privacy Protection Principle 7: Accuracy / "Précision suffisante et adéquate"

It is to the mutual benefit of all parties to a learning transaction, and also a best practice, to ensure that any and all recorded information pertaining to a learning transaction be as timely, accurate, complete, up-to-date, etc., as possible. Accuracy of recorded information is an essential component of "integrity[9]" which is a major asset of any organization.

[9] It is noted that an organization which (1) does not have policies and auditable procedures in place, as part

No organization should keep recorded information on its learning transactions or its clients which is not accurate or out-of-date.

8. Privacy Protection Principle 8: Safeguards / "Application du principe de précaution »

This 8th privacy protection principle pertains to ensuring that the organization has in place policies, operational controls and practices to ensure that its policies pertaining to the retention, storage, preservation or destruction, confidentiality, integrity, continuity and availability of its personal information, as well as the processing, reproduction, distribution, sharing or other handling of such personal information is "safeguarded" in compliance with applicable "information law" requirements.

Personal information shall be protected by operational procedures and safeguards appropriate to the level of sensitivity of such recorded. And the organization shall have in place (and tested) measures in support of compliance of compliance with privacy protection requirements of applicable jurisdictional domains, (as well as any other external constraints which may apply such measures as are appropriate to ensure that all applicable legal requirements are supported such as generic ILCM requirements).

9. Privacy Protection Principle 9: Openness / "Transparence"

The principle of "openness" pertains to the privacy protection requirement that any organization which collects and uses personal information shall be fully transparent in its use of such personal information. This means that all of its policies and operational practices pertaining to the collection, use, and management of any personal information shall be made readily and publicly available, free of charge, and via various means and media of communication.

Therefore, an organization shall have and make readily available to any Person[10] specific information about its policies and practices pertaining to the management and interchange of personal information under its control.

10 Privacy Protection Principle 10: Individual Access / "droit d'accès individuel»

An individual has the right to know whether or not an organization has personal information under its control[11] on or about that individual**.**

---

of its overall governance, to ensure that the recorded information on which its decisions and commitments are made; (2) does not have the required level of "integrity" (e.g. timeliness, accuracy, being-up-to data, etc.,; and (3) ensures that all its recorded information, does not meet these criteria is expunged (unless required to be retained due to applicable external constraints), may well find itself (and particular its officers) being subject to legal action for not exercising stewardship, due diligence, damages, etc.,, for not implementing these requirements (which in turn form part of the implementation of ICLM principles).

[10] "Person" is used here, instead of individual so that other (potential) parties to a learning transaction, (e.g., organizations and public administrations) need to have access to an organization's privacy protection policies, practices and related information.

[11] The use of "under its control" covers the fact that the organization may engage agents, third parties, other parties to a business transaction and thus provide them with personal information. However, the LET provider retains control of all its recorded information including personal information.

A key component of privacy protection requirements is that an individual shall be able to enquire of any organization (private or public sector) whether or not that organization has and maintains personal information about that individual, anywhere in the record/information management systems of that organization.

11. Privacy Protection Principle 11: Challenging Compliance / "droit de mise à niveau et mise à jour »

Challenging compliance is a key privacy protection principle. It pertains to the right of an individual to question and thus challenge whether or not: (1) an organization has under its control (or maintains on behalf of other organizations) personal information on the individual; and, (2) if it does, that such personal information is accurate, timely, and relevant to the nature of the informed consent provided by that individual.

Depending on the privacy protection requirements of the applicable jurisdictional domain, an individual may have the right to:

(a) Challenge compliance directly with the organization to whom the challenge is directed;
(b) direct such a challenge, (e.g., complaint) to a privacy or data protection commissioner/ombudsman as provide for in the jurisdictional domain; or,
(c) various combinations of (a) or (b) above".

2. Need for an IT-platform Neutral Approach

Two possible approaches:

A. Keep developing new standards as technology changes, i.e. technology-based implementations standards

B. Differentiate between 1) ongoing user operational requirements (including legal & regulatory) oriented standards; and, 2) ICT functional support services oriented standards

OPTION A – Advantages & Disadvantages

Advantages: Standard focused on a particular ICT relatively quick to develop, market and implement. Will have a distinct market. Are mostly "supplier driven".

Disadvantages: As the technology changes, the standard needs to change. Often difficult to link to user requirements and applications. Often not interoperable with other ICT standards nor harmonized with them. Have a tendency to "lock in" users to a particular ICT. Have a tendency to advocate a technology driven approach rather than user requirements driven approach.

OPTION B – Advantages and Disadvantages

Advantages: Are user requirements driven. User operational requirements, from an IT-platform neutral perspective, are quite constant as are associated legal and regulatory requirements which apply. One can differentiate between generic and sector-specific standards using the former to build the latter. Standards once developed are more permanent being based on user requirements & best practices.

Disadvantages: Require more up-front work and resources. At times take longer to develop due to effort necessary to identify and specify generic user requirements and best practices in the particular user sector. Incorporating or structuring a standard to be able to support applicable legal & regulatory requirements presents another challenge.

The new ITLET & Privacy Protection standard, will contain a Clause 1.n titled *"IT-system environmental neutrality"*

"This standard does not assume nor endorse any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, syntax, computing platform, or any technology required for implementation , i.e., it is information technology neutral. At the same time, this standard maximizes an IT-enabled approach to its implementation and maximizes semantic interoperability."

NOTE: Privacy protection requirements are IT-platform neutral

3. Importance and role of concepts, their definitions and associated terms: Back to basics - but in an IT-enabled manner + Maximize Use of Existing Standards

Work on the development of the "ITLET and Privacy Protection" standard requires the identification and/or development of key concepts and their definitions.

Concepts are the basic building block of any standard. Thus "Clause 3 Definitions[12]" in an international ISO standard is one of its most important Normative clauses. The other Normative Clauses use and expand on the Clause 3 defined concepts. Standard development is an exercise in consensus-building among the participating parties.

Without agreed upon core concepts and their definitions, there basically cannot be a "standard". It is therefore of primary importance

- that each concept has a clearly stated and unambiguously stated definition (with Notes[13] & Examples[14] where necessary or deemed useful);

- that all the concepts used in a standard interwork which each other, there are no tautologies (= circularities among the concepts and their definitions), and that together they from a unified whole;

- in order to minimize ambiguity in the definitions and associated terms in a standard, they must be made available in at least one other language other then English. This is necessary to avoid misinterpretation. This is also necessary in order to be able to support multilingual Human Interface Equivalents (HIEs).[15]

- that the choice of the label, i.e., term, associated with the definition of the concept, must be made with care. One must also minimize the problem of "polysemy", i.e. the use of the same term for different concepts and their definitions.

One cannot assume that there exists a "common understanding" world-wide for a specific concept, often represented by its label (term). And even if such a common understanding exists, it is still necessary to formally and explicitly (re-affirm) such a

[12] Sometimes in an ISO standard the Clause containing the definitions may be numbered as Clause 2 or 4 (or "n").

[13] "NOTES" are often used to capture primary properties or behaviours stated as rules in the standard itself. This is because ISO requires that a definition be stated as a single sentence.

[14] "EXAMPLES" are used where this is deemed necessary to understand the context of use of the concept and its definition.

[15] For the definition of HIE see the definitions document JTC1/SC36/WG305f which is being revised to place these in a LET & learning transaction context. Working Group 7 of ISO/IEC JTC1/SC36 has launched a multipart "Access for All" standards project ISO/IEC 20016 titled" …*Language Accessibility and Human Interface Equivalencies (HIEs) in e-Learning applications: Principles, Rules, and Attributes of Semantic Data*:. Here work is underway on "*Part 1: Framework and Reference Model*"

common understanding, i.e. by it being so stated in normative Clause 3 Definitions in a an ISO standard.

Because of the widespread use of the Internet by individuals, it is important that concepts and their definitions be both

1) IT-platform neutral; and,
2) IT-enabled, i.e. being able to map to the use of both virtual & real worlds.

In the pre-standard development phase of the ISO/IEC JTC1/SC36 re "ITLET & Privacy Protection", i.e. though its Ad-Hoc on Privacy (see document JTC1/SC36 N1737), 80+ ISO standards were identified as being relevant to this standards development project. Thus a key principle to be applied is

"**Maximize Use of Existing Standards where applicable & relevant" (= Do Not Re-invent the Wheel")**

4. Who & What are we talking about? What is a "Person"? [and its sub-types "individual", "organization" & "public administration"]

? In the dematerialized world of ICT and the Internet what is a "Person", i.e. as the entity able to make commitments, have rights and obligations, capable of being held accountable for, etc.

? how do we deal with the fact that in law, human beings, can have 1) the role of "natural person" singly and simply by themselves, i.e. as a "personne physique"; and/or, 2) combine with other human beings to form an organization, i.e., "personne morale"?

This issue has been resolved in ISO/IEC Open-edi and eBusiness standards. This is summarized in the following figure followed by the existing ISO definitions (in English & French) for the concepts identified in Figure B below[16].

n

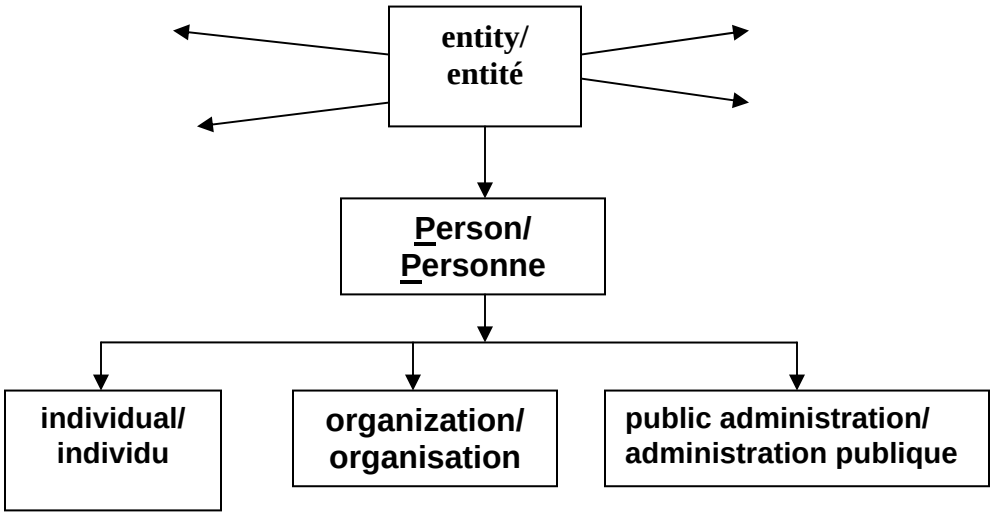


Figure B: entity->Person & its 3 sub-types "individual", organization" and "public administration"

n

Figure B illustrates that a "Person" is modelled as a very particular and unique type of "entity". "Person" is capitalized to denote it as a specific and defined ISO concept which includes both natural persons and legal persons. It is important to note that a "Person the only type of entity that is able to make a "commitment / engagement". (see ISO definitions below).

---

[16] For a more detailed explanation and associated rules of Figure B and text presented here, see Clause 6 "*Rules Governing the Person component",* and in particular Clause 6.2.7 *"Person and external constraints: individual, organization, and public administration"* in ISO/IEC 15944-1:2010 "*Information technology — Business agreement semantic descriptive techniques — Part 1: Operational aspects of Open-edi for implementation Technologies de l'information — Techniques descriptives sémantiques des accords d'affaires — Partie 1: Aspects opérationnels de l'EDI ouvert pour application* (E) + (E/F definitions), 2nd ed.

Figure B also illustrates that a “Person” in turn has three distinct sub-types, namely “Individual”, “organization” and “public administration”. From an object-oriented modelling perspective, the three sub-types of Person inherit all the properties and behaviours of a Person.

n

ISO/IEC 2382-17:1999 (17.02.05)	entity	99	any concrete or abstract thing that exists, did exist, or might exist, including associations among these things EXAMPLE A person, object, event, idea, process, etc. NOTE An entity exists whether data about it are available or not.	entité	01	tout objet ou association d'objets, concret ou abstrait, existant, ayant existé ou pouvant exister EXEMPLE Personne, événement, idée, processus, etc. NOTE Une entité existe que l'on dispose de données à son sujet ou non.

ISO/IEC 14662: 2004 (3.24)	Person	99	**entity**, i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make **commitment**(s), assume and fulfill resulting obligation(s), and able of being held accountable for its action(s) NOTE 1 Synonyms for "legal person" include "artificial person", "body corporate", etc., depending on the terminology used in competent jurisdictions. NOTE 2 "Person" is capitalized to indicate that it is being used as formally defined in the standards and to differentiate it from its day-to-day use. NOTE 3 Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common subtypes of Person, namely "individual", "organization", and "public administration".	Personne	02	**entité**, c.-à-d. une personne physique ou morale, reconnue par la loi comme ayant des droits et des devoirs, capable de faire des **engagements**, d'assumer et de remplir les obligations résultantes, et capable d'être tenue responsable de ses actions NOTE 1 Parmi les synonymes de «personne morale», on trouve «personne juridique», «personne fictive», «corporation», etc., selon la terminologie utilisée par les juridictions compétentes. NOTE 2 « Personne » prend la majuscule pour indiquer que ce terme est utilisé tel que défini officiellement dans les normes et pur le différencier de son usage ordinaire. NOTE 3 Les exigences minima et communes applicables aux transactions d'affaires obligent souvent à faire une différence entre les trois sous-catégories communes de « Personne », notamment « individu », « organisation », « administration publique».

ISO/IEC 15944-1:2002 (3.28)	individual	99	**Person** who is a human being, i.e., a natural person, who acts as a distinct indivisible **entity** or is considered as such	individu	01	**Personne** qui est un être humain, c-à-d. une personne physique, qui agit à titre d'**entité** indivisible distincte ou qui est considérée comme telle

ISO/IEC	organ	99	unique framework of authority	organis	02	cadre unique d'autorité dans lequel une

6523-1:1998 (3.1)	ization		within which a person or persons act, or are designated to act, towards some purpose NOTE The kinds of organizations covered by this International Standard include the following examples: EXAMPLE 1 An organization incorporated under law. EXAMPLE 2 An unincorporated organization or activity providing goods and/or services including: 1) partnerships; 2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals; 3) sole proprietorships 4) governmental bodies. EXAMPLE 3 Groupings of the above types of organizations where there is a need to identify these in information interchange.	ation		ou plusieurs personnes agissent ou sont désignées pour agir afin d'atteindre un certain but NOTE Les types d'organisations couverts par la présente partie de l'ISO/CEI 6523 comprennent par exemple les éléments suivants: EXEMPLE 1 Organisations constituées suivant des formes juridiques prévues par la loi. EXEMPLE 2 Autres organisations ou activités fournissant des biens et/ou des services, tels que: 1) sociétés en participation; 2) organismes sociaux ou autres à but non lucratif dans lesquels le droit de propriété ou le contrôle est dévolu à un groupe de personnes; 3) entreprises individuelles; 4) administrations et organismes de l'état. EXEMPLE 3 Regroupements des organisations des types ci-dessus, lorsqu'il est nécessaire de les identifier pour l'échange d'informations.

ISO/IEC 15944-1:2002 (3.54)	public administration	99	**entity**, i.e., a **Person**, which is an **organization** and has the added **attribute** of being authorized to act on behalf of a **regulator**	administration publique	01	**entité**, c.-à-d. une **Personne**, qui est une **organisation** et a l'**attribut** supplémentaire d'être autorisé à agir au nom d'une **autorité de réglementation**

ISO/IEC 14662:2004 (3.5)	commitment	99	making or accepting of a right, obligation, liability or **responsibility** by a **Person** that is capable of enforcement in the **jurisdictional domain** in which the **commitment** is made	engagement	01	création ou acceptation d'un droit, d'une obligation, d'une dette ou d'une **responsabilité** par une **Personne** qui est apte à appliquer le **domain jurisdictionel** conformément à laquelle l'**engagement** est pris

5. What are the key public policy requirements as rights of individuals impacting the use of ICT (of which "privacy protection" is part?)

"Privacy protection" is a human right, i.e., only natural persons, have privacy protection right. Organizations and public administrations are "legal persons" and do not have privacy protection rights. They have privacy protection obligations.

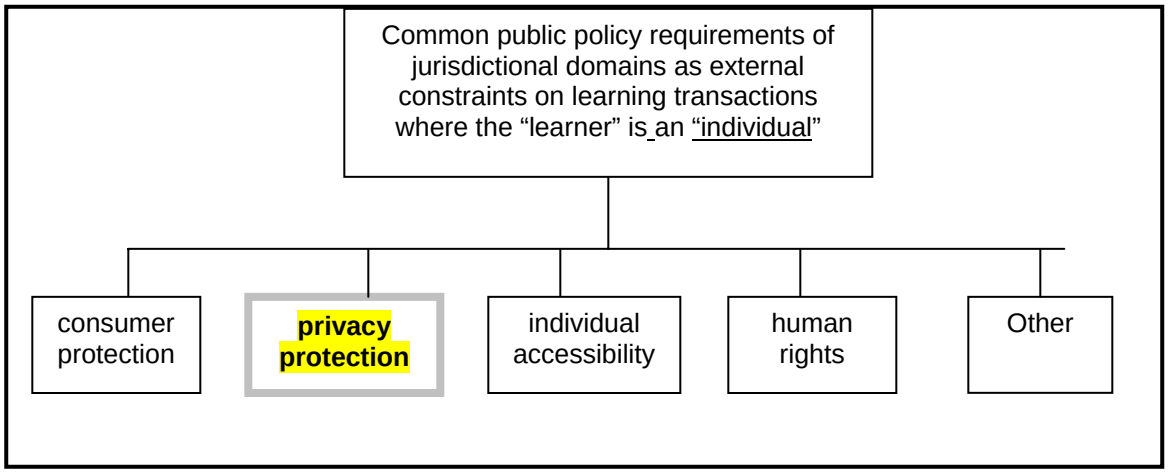
Organization cans confidentiality requirements & obligations based on contractual agreements. Public administration can have "secrecy requirements[17]" in addition to confidentiality requirements for their recorded information (e.g. re national defence, Cabinet secrecy, national security,, economic sensitivity, etc.).

It is therefore imperative that one make a clear distinction between 1) "privacy protection" as a human right; and 2) confidentiality, secrecy, etc. which have different and other sources of generic civil and common law requirements (in public and private law) of applicable jurisdictional domains.

"Privacy protection" is part of a family of international and domestic law pertaining to rights of individuals in their interactions with organizations and public administrations. Other key examples include "consumer protection" and "individual accessibility"[18]. They are part of a family of external constraints of jurisdictional domains on organizations and public administrations which apply when these interact with "individuals".

In an ISO context, this family has been labelled as "public policy". This ISO approach is summarized in Figure C. The relevant ISO definitions (in English & French), follow below Figure C.

n



[17] These are usually specified by jurisdictional domains in their Privacy or Data Protection legislation itself or through reference to other applicable legislation such as Freedom of Information, Access to Information, Official Secrets, etc., Acts.

[18] Here the UN "*Convention of Rights of persons with disabilities and optional protocol"* (A/64/128) / ONU "Convention relative aux droits des personnes handicapées" < http://www.un.org/disabilities >. This UN Convention is a major source in the development by Working Group 7 of ISO/IEC JTC1/SC36 of the multipart "Access for All" standards project ISO/IEC 20016 titled" …*Language Accessibility and Human Interface Equivalencies (HIEs) in e-Learning applications: Principles, Rules, and Attributes of Semantic Data*:. Here development work is underway on "*Part 1: Framework and Reference Model"*

n

This Figure C is based on that found in both ISO/IEC 15944-5:2008 and ISO/IEC FDIS 15944-8:2010. (For the titles of these two standards see Annex A below).

n

ISO/IEC 15944-5:2008 (3.113)	public policy	99	category of **external constraints** of a **jurisdictional domain** specified in the form of a right of an **individual** or a requirement of an **organization** and/or **public administration** with respect to an **individual** pertaining to any exchange of **commitments** among the parties concerned involving a good, service and/or right including information management and interchange requirements NOTE 1 Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a business transaction, i.e., planning, identification, negotiation, actualization and post-actualization. {See further Clause 6.3 "Rules governing the process component" in ISO/IEC 15944-1:2002} NOTE 2 It is up to each jurisdictional domain to determine whether or not the age of an individual qualifies a public policy requirement, (e.g., those which specifically apply to an individual under the age of thirteen (13) as a "child", those which require an individual to have attained the age of adulthood, (e.g., 18 years or 21 years of age) of an individual to be able to make commitments of a certain nature. NOTE 3 Jurisdictional domains may have consumer protection or privacy requirements which apply specifically to individuals who are considered to be "children", "minors", etc., (e.g. those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain).	politique publique	01	catégorie de **contraintes externes** d'un **domaine juridictionnel** spécifié sous la forme d'un droit d'un **individu** ou d'une exigence exercée sur une **organisation** et/ou une **administration publique** en ce qui concerne un **individu** relatif à tout échange d'**engagements** entre les parties concernées à propos d'un bien, d'un service et/ou d'un droit, y compris les exigences en matière de gestion de l'information et d'échange NOTE 1 Des exigences en matière de politique publique peuvent s'appliquer à l'une ou à toutes les combinaisons des activités fondamentales touchant une transaction d'affaires, c.-à.-d. la planification, l'identification, la négociation, l'actualisation et la post-actualisation. {Voir plus loin la Clause 6.3 « Règles régissant la composante de processus » dans l'ISO/IEC 15944-1:2002} NOTE 2 Il appartient à chaque domaine juridictionnel de déterminer si l'âge d'un individu qualifie une exigence en matière de politique publique (par ex. celles qui s'appliquent spécifiquement à un individu de moins de treize (13) ans en tant qu'« enfant », celles qui exigent qu'un individu ait atteint l'âge adulte, (par ex. 18 ou 21 ans), pour qu'un individu soit en mesure de prendre un engagement d'une certaine nature. NOTE 3 Des domaines juridictionnels peuvent avoir des exigences en matière de protection du consommateur ou de la vie privée qui s'appliquent spécifiquement à des individus qui sont considérés comme des « enfants » ou des « mineurs », etc. (c.-à.-d. ceux qui n'ont pas encore atteint leur 18 è ou 21è anniversaire de naissance conformément aux règles du domaine juridictionnel applicable).

ISO/IEC 15944-	consumer	99	set of **external constraints** of a **jurisdictional domain** as rights of	protection du	01	ensemble de **contraintes externes** d'un **domaine juridictionnel** comme

5:2008 (3.33)	protection		a **consumer** and thus as obligations (and possible liabilities) of a **vendor** in a **business transaction** which apply to the good, service and/or right forming the **object** of the **business transaction** (including associated information management and interchange requirements including applicable (sets of) **recorded information**) NOTE 1 Jurisdictional domains may restrict the application of their consumer protection requirements as applicable only to individuals engaged in a business transaction of a commercial activity undertaken for personal, family or household purposes, i.e., they do not apply to natural persons in their role as "organization" or "organization Person". NOTE 2 Jurisdictional domains may have particular consumer protection requirements which apply specifically to individuals who are considered to be a "child" or a “minor”, (e.g., those individuals who have not reached their thirteenth (13) birthday). NOTE 3 Some jurisdictional domains may have consumer protection requirements which are particular to the nature of the good, service and/or right being part of the goal of a business transaction.	consommateur		droits d’un **consommateur** et ainsi comme obligations (et responsabilités éventuelles) d’un **fournisseur** dans une **transaction d’affaires** qui s’applique au bien, au service et/ou droit faisant l’**objet** de la **transaction d’affaires** (y compris les exigences en matière de gestion et l’échange de l’information qui s’y rattachent, dont l’(ou l’ensemble des) **information enregistrée** applicable NOTE 1 Des domaines juridictionnels peuvent restreindre l’application de leurs exigences en matière de protection du consommateur comme applicables uniquement aux individus participant à une transaction d’affaires de nature commerciale entreprise à des fins personnelles, familiales ou domestiques, c.-à.-d. qu’ils ne s’appliquent pas aux personnes physiques dans leur rôle d’ « organisation » ou de « Personne d’organisation ». NOTE 2 Des domaines juridictionnels peuvent avoir des exigences particulières en matière de protection du consommateur qui s’appliquent spécifiquement à un individu considérés comme un « enfant » ou un « mineur » (par ex. les individus n’ayant pas encore atteint leur treizième anniversaire de naissance). NOTE 3 Certains domaines juridictionnels peuvent avoir des exigences en matière de protection du consommateur propres à la nature du bien, du service, et/ou du droit faisant l’objet d’une transaction d’affaires.

ISO/IEC 15944-5:2008 (3.109)	privacy protection	99	set of **external constraints** of a **jurisdictional domain** pertaining to **recorded information** on or about an identifiable **individual**, i.e., **personal information**, with respect to the creation, collection, management, retention, access and use and/or distribution of such **recorded information** about that **individual** including its accuracy, timeliness, and relevancy NOTE 1 Recorded information collected or created for a specific purpose on an identifiable	protection de la vie privée	01	ensemble de **contraintes externes** exercées sur un **domaine juridictionnel** relatives à l’**information enregistrée** ou à propos d’un **individu** identifiable, c.-à.-d. de l’**information personnelle**, en ce qui concerne la création, la collecte, la gestion, la rétention, l’accès et l’utilisation et/ou la distribution d’une telle **information enregistrée** relative à cet **individu** , y compris son exactitude, son opportunité et sa pertinence NOTE 1 L’information enregistrée

			individual, i.e., the explicitly shared goal of the business transaction involving an individual shall not be used for another purpose without the explicit and informed consent of the individual to whom the recorded information pertains. NOTE 2 Privacy requirements include the right of an individual to be able to view the recorded information about him/her and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date. NOTE 3 Where jurisdictional domains have legal requirements which override privacy protection requirements these must be specified, (e.g., national security, investigations by law enforcement agencies, etc.).			recueillie ou créée dans un but spécifique concernant un individu identifiable (c.-à.-d. le but partagé et explicite de la transaction d'affaires concernant un individu) ne peut être utilisée dans un autre but sans le consentement explicite et informé de l'individu auquel l'information enregistrée se rapporte. NOTE 2 Les exigences en matière de vie privée incluent le droit d'un individu de pouvoir examiner l'information enregistrée le (ou la) concernant, et de demander d'y apporter des corrections afin de s'assurer que l'information enregistrée est exacte et à jour. NOTE 3 Lorsque des domaines juridictionnels ont des exigences légales qui ont préséance sur les exigences en matière de protection de la vie privée (par ex. la sécurité nationale, les enquêtes policières, etc.), ils doivent être spécifiés.

ISO/IEC 15944-5:2008 (3.60)	individual accessibility	99	set of **external constraints** of a **jurisdictional domain** as rights of an **individual** with disabilities to be able to use IT systems at the human, i.e., user, interface and the concomitant obligation of a **seller** to provide such adaptive technologies NOTE Although "accessibility" typically addresses users who have a disability, the concept is not limited to disability issues. EXAMPLE Examples of disabilities in the form of functional and cognitive limitations include: - people who are blind; - people with low vision; - people with colour blindness; - people who are hard of hearing or deaf, i.e., are hearing impaired; - people with physical disabilities; - people with language or cognitive disabilities.	accessibilité individuelle	01	ensemble de **contraintes externes** d'un **domaine juridictionnel** comme droits d'un **individu** atteint de déficience d'être capable d'utiliser des systèmes TI au niveau de l'interface humaine, c.-à.-d. utilisateur, et l'obligation concomitante d'un **vendeur** d'offrir ce type de technologies adaptatives NOTE Bien que l'« accessibilité » s'adresse typiquement aux utilisateurs qui ont une déficience, le concept ne se limite pas aux questions de déficience. EXEMPLE Comme exemples de déficiences sous formes de limitations fonctionnelles et cognitives, on trouve : - les personnes aveugles; - les personnes à basse vision; - les personnes atteintes d'achromatopsie; - les personnes sourdes ou ayant une déficience auditive; - les personnes atteintes de déficience physique; - les personnes atteintes de déficience linguistique ou cognitive.

Requirements of jurisdictional domains on Persons such as “public policy”, “consumer protection”, privacy protection”, “individual accessibility”, evidentiary requirements, those of a records-keeping nature, etc., have a strong “information law” component. Most laws & regulations which are of an information law nature (or have a strong information law component) are independent of the good, service and/or right being provided.

The ISO definition for “<u>information law / loi sur l’information</u>”

ISO/IEC 15944-8:2010 (3.62)	Information law	99	any law, regulation, policy, or code (or any part thereof) that requires the creation, receipt, collection, description or listing, production, retrieval, submission, retention, storage, preservation or destruction of **recorded information**, and/or that places conditions on the access and use, confidentiality, privacy, integrity, accountability(ies), continuity and availability of processing, reproduction, distribution, transmission, sale, sharing or other handling of **recorded information**	loi sur l’information	01	toute loi, règlement, politique ou code (ou partie de ceux-ci) qui exige la création, la réception, la collecte, la description ou le listage, la production, l’extraction, la soumission, la rétention, le stockage, la préservation ou la destruction de l’**information enregistrée**, et/ou qui impose des conditions à l’accès et à l’utilisation, à la confidentialité, à la protection de la vie privée, à l’intégrité, aux responsabilités, à la continuité et à la disponibilité du traitement, de la reproduction, de la distribution, de la transmission, de la vente, du partage ou tout autre manipulation de l’**information enregistrée**

Even laws which are sector specific**,** pertains to the extraction manufacturing, trade, etc., of a specified good (including commodities), services, and/or rights have “information law” components, i.e. require the creation or collection of recorded information, its retention, transmission to a public administration, made publicly available, etc.

6. What is “recorded information”? What is “personal information”?

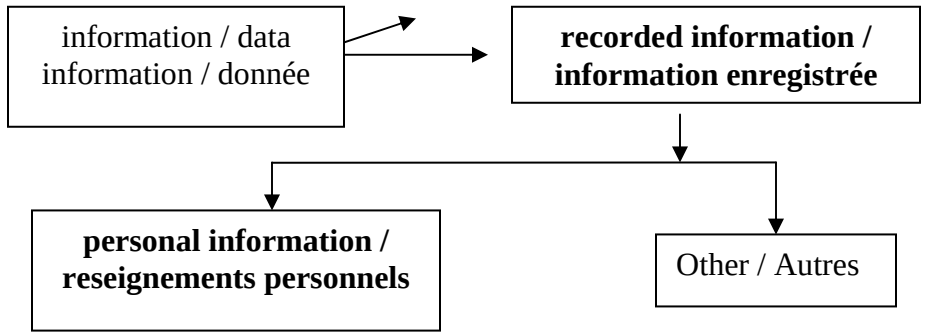
Different concepts and definitions exist for “data”, “information”, “records”, “documents”, etc. They exist in both in ISO standards and in laws and regulations of an “information law” nature.

At the same time, the making of a “commitment” can be done verbally as well as through “reducing the same in writing”. However, from an ICT perspective, if the information is not recorded it does not exist (in either the virtual world or the real world). If information is not recorded, it cannot be accessed, retrieved, viewed/used, managed, protected, etc. (See further Clause 6.4.1 and Annex G.3 & G.4 in ISO/IEC 15944-1).

In addition, not all recorded information is “personal information”. Only recorded information on or about an identifiable individual is “personal information”.

Figure D below summarizes this (and the existing applicable ISO definitions (in English and French) follow the figure).

n



n

ISO/IEC 15944-1:2002 (3.56)	recorded information	99	any **information** that is recorded on or in a **medium** irrespective of form, recording **medium** or technology used, and in a manner allowing for storage and retrieval NOTE 1 This is a generic definition and is independent of any ontology, (e.g., those of "facts" versus "data" versus "information" versus "intelligence" versus "knowledge", etc.). NOTE 2 Through the use of the term "information," all attributes of this term are inherited in this definition. NOTE 3 This definition covers:	information enregistrée	02	toute **information** enregistrée sur ou dans un **support** quelle que soit sa forme, le **support** de stockage ou la technologie utilisés, et de façon à permettre son stockage et son extraction NOTE 1 Cette définition est générique et indépendante de toute ontologie, (par exemple le point de vue des «faits» par rapport aux «données», à «l'information», aux «renseignements», à la «connaissance», etc.). NOTE 2 Dans l'utilisation du terme «information», tous les attributs de ce terme sont hérités dans cette définition. NOTE 3 Cette définition couvre les

			(i) any form of recorded information, means of recording, and any medium on which information can be recorded; and, (ii)all types of recorded information including all data types, instructions or software, databases, etc.			élément suivants : (i)toute forme d'information enregistrée, tout moyen d'enregistrement, et tout support sur lequel l'information peut être enregistrée; et, (ii) tous types d'information enregistrée, y compris tous les types de données, instructions ou logiciels, bases de données, etc.

ISO/IEC 15944-5:2008 (3.103)	personal information	99	any information about an identifiable **individual** that is recorded in any form, including electronically or on paper NOTE Some examples would be recorded information about a person's religion, age, financial transactions, medical history, address, or blood type.	renseig ne-ments person nels	01	tout renseignement au sujet d'un **individu** identifiable, qui est enregistré sous une forme quelconque, y compris électroniquement ou sur papier NOTE Cela comprend, par exemple, les information enregistrée à propos de la religion, de l'âge, des opérations financières, du passé médical, de l'adresse ou du groupe sanguin de quelqu'un.

7. From the ISO/IEC 14662 Open-edi Reference Model and "business transaction to "learning transaction" and "learning collaboration space": "individual learner" & "LET provider" as the key role players

A very significant aspect of the ISO/IEC 14662 "*Information technology -Open-edi Reference Model/ Technologies de l'information – Modèle de reference EDI-ouvert",* is that (a) it focuses on a business transaction" as a whole; and (b), from a standards development perspective. ISO/IEC 14662 is very important in that (2) it is transaction-based; and, (2) that these transactions pertain to and support the making of commitments among Persons. Further the Open-edi Reference Model addresses the totality of standardisation requirements in support of business transaction, and acknowledges that these need to be viewed from two different but complimentary perspectives.[19] The Open-edi Reference Model therefore makes a clear distinction between two perspectives, namely,

1. the Business Operational View (BOV) / Vue opérationnelle des affaires; and,
2. the Functional Services View (FSV) / Vue fonctionnelle des services

Figure E below is a copy of Figure 1 in ISO/IEC 14662.
n

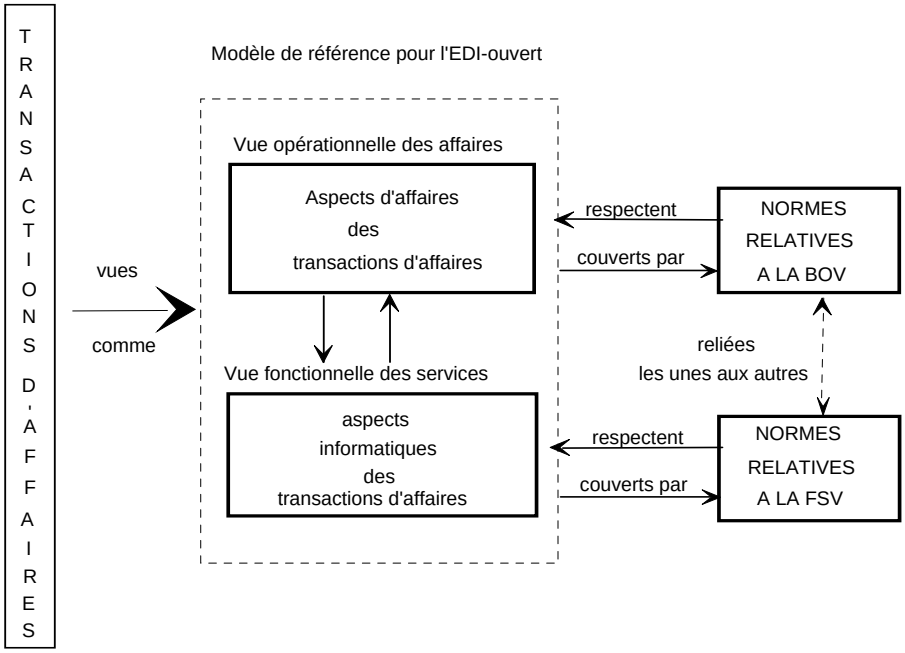


Figure 1 – Environnement de l'EDI-ouvert

[19] The ISO/IEC 14462 Open-edi Reference Model serves as the basis of the 2000 Memorandum of Understanding (MOU) between ISO, IEC, ITU and the UN/ECE on concerning standardization in the field of electronic business (see< http://www.itu.int//ITU-T/e-business/files/mou.pdf >

Applying the Open-edi reference Model and based on the premises that personal information

1. personal information is something of value
2. the individual learner must give informed consent before its personal information can be collected and used by an organization or public administration;
3. there are rules governing the use, disclosure, retention, accuracy, safeguards, etc., that apply to personal information;
4. that in fact the organization or public administration is required by law to make a commitment to comply with privacy protection requirements,

one can view privacy protection requirements as a form of commitment exchange imposed on organization and public administrations with respect to the personal information of an individual learner.

In addition, the purpose and goal of the exchange of personal information between the individual learner and the organization must be stated and agreed to. Personal information collected for one purpose, i.e., as a mutually agreed to common goal, may not be used for another purpose without the individuals consent.

Therefore one can model these exchanges of personal information between the individual learner and a LET provider pertaining to a specified goal as “learning transactions” and apply the Open-edi Reference Model, illustrated in Figure F as follows n

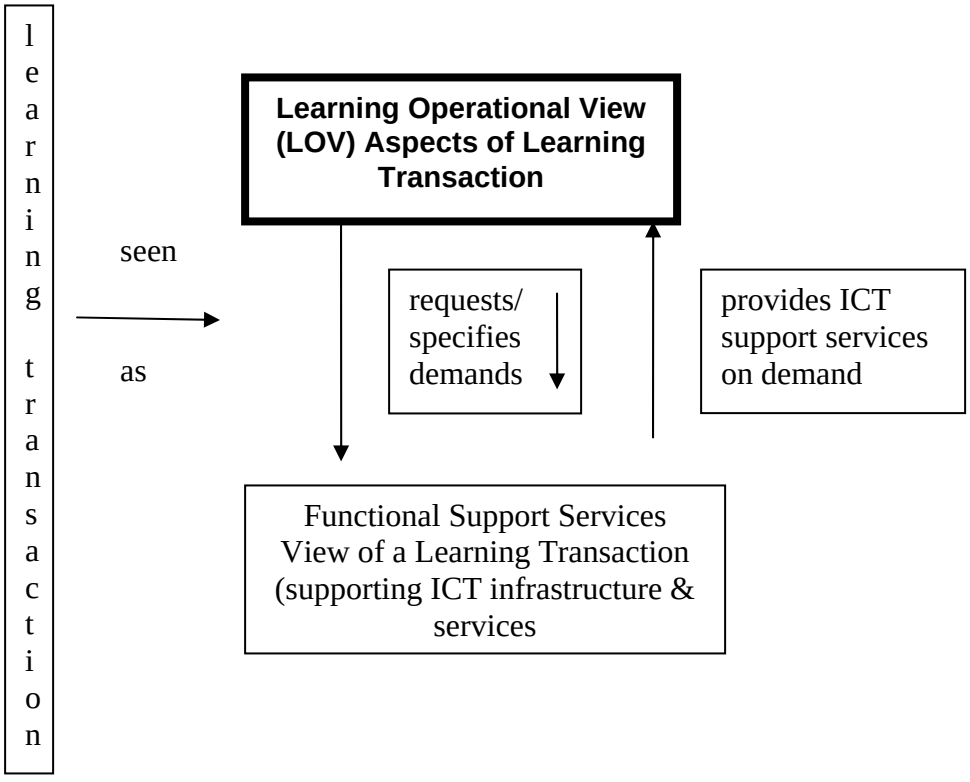


Figure F - Learning Transaction Model in Privacy Protection Environment

The initial focus of the development of ISO/IEC 19187-1 will be on the development of the "Learning Operational View" aspects.

The draft working definition of "learning transaction" is;

learning transaction:

predefined set of activities and/or **processes** among **Persons** which is initiated by a **Person,** i.e. in the role of **individual learner**, **LET provider** and/or **regulator**, involving the exchange of **recorded information**, to accomplish an explicitly stated learning goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit

NOTE 1: A learning transaction is realized through the exchange of verbal and recorded information and directed towards some mutually agreed upon goal extending over a period of time.

NOTE 2 A learning transaction may be internal constraints-based or external constraints-based. A primary example of an external constraint-based learning transaction is that of jurisdictional domains governing minimum levels of schooling, (e.g., K-12).

NOTE 3 A learning transaction can be on a for-a-fee or for-free basis.

NOTE 4 A LET provider can offer a learning transaction and operate on either a for-profit or not-for-profit basis.

NOTE 5 A learning transaction can consist of two or more learning transaction, each having their own stated (detailed) goal, yet at the same time forming part of a (overall goal).

[ISO/IEC 29187-1 (3.nn)]

The three key roles in a business transaction are "buyer", "seller" and "regulator". In a learning transaction in a privacy protection environment, these would become "individual learner", "LET provider" and regulator.

Figure H below summarizes this approach. To this we have also added the "consumer protection" requirements environment

Environment	**Role (in transaction**	**Role (in transaction)**	**Role (in transaction)**
Generic	**user**	**supplier**	**(regulator)**
business transaction (generic)	buyer	seller	regulator
learning transaction (Privacy protection)	individual learner	LET provider	regulator
consumer protection	consumer	vendor	regulator

ISO/IEC 2382-36:2009 "*Information technology – Vocabulary- Part 36: Learning, Education, and Training / Technologie de l'information – Vocabulaire – Partie: Apprentissage, education et formation*" defines "learner" as

learner
entity that learns

apprenant
entité qui apprend
[ISO/IEC 2382-36 (36.02.01)]

Since privacy protection requirements do not apply to any kind of entity but only to individuals, the concept and definition of "individual learner" is being introduced with the following draft definition:

individual learner:

learner who participates as an **individua**l in a **learning transaction**

[French language equivalent ?????]

[ISO/IEC 29187-1 (3.nn)]

Similarly, within a LET environment, the use of "seller" & "vendor" are not that favoured. In any case these concepts and their terms are already "taken" and it is important to have a distinct concept, definition and associated term for use in a LET environment. Thus we have the following draft working definition:

LET provider
Person, as **organizatio**n or **public administration** which provides a good, service, and/or right in the fields of learning, education or training as part of a **learning transaction**

[French language equivalent ?????]

[ISO/IEC 29187-1 (3.nn)]

Here one notes that the role of "regulator" and its definition is essentially generic in nature and applies in any environment or sector. Amending the existing definition for "regulator / autorité de réglementation" and substituting provides the following definition for this concept.

Source	Term	G	ISO English Amended for ITLET + Privacy protection environment	Terme	G	ISO French Term and definition yet to be amended to ITLET & Privacy protection environment
Adapted from ISO/IEC 15944-	regulator (in learning transaction)	99	**Person** who has authority to prescribe **external constraints** which serve as **principles**, policies or **rules** governing or prescribing the behaviour of **Persons**	autorité de réglemen-tation	02	**Personne** autorisée à prescrire des **contraintes externes** qui servent de **principes**, de politiques ou de **règles** régissant ou prescrivant le comportement

1:2002 (3.59)			involved in a **learning transaction** as well as the provisioning of goods, services, and/or rights interchanged			des **Personnes** concernées par une **transaction d'affaire**, ainsi que la fourniture des biens, services et/ou droits échangés

The last point to be made here is that a learning transaction between an "individual learning" and a "LET provider" needs to be viewed not from the perspective of each of these two parties but one that is common to both, i.e. as an independent view of their common "collaboration space"

Figure I below is adapted from Figure 5 in ISO/IEC 15944-5 and Figure 3 in ISO/IEC 15944-8**.**

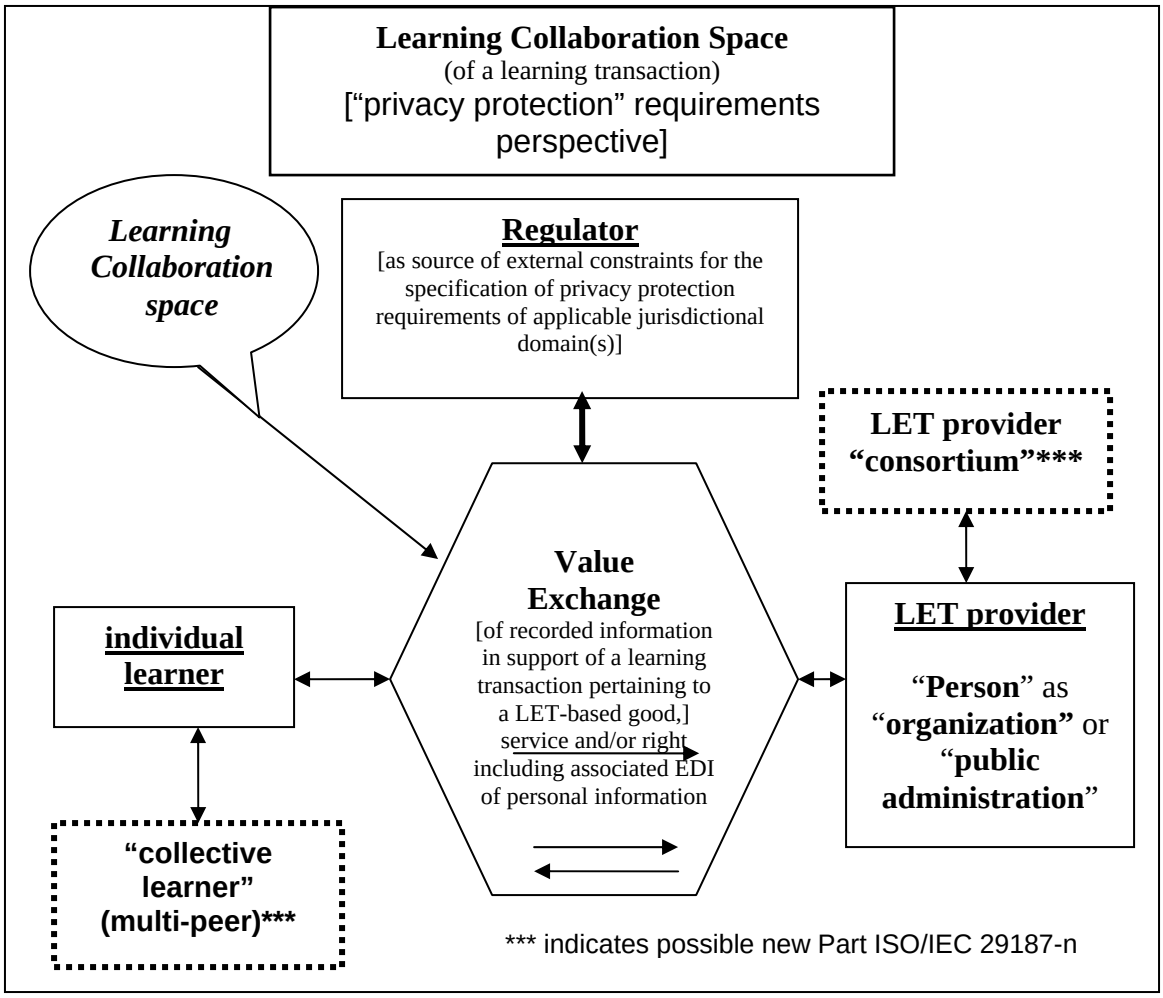


Figure I –Learning collaboration space (of a learning transaction) including the role of a regulator

n

With respect to Figure I , one should note that it is constricted to identify the more primitive aspects only. Dotted lines are used for “boxes” to indicated the next level of granularity. Depending on the level of granularity others aspects can be added as well.

For example, the roles of Persons as “agent” and “third” parties[20]” along with the associated rules, can also be modelled in a learning transaction. Depending on the nature and goal of the learning transaction, an individual learner may use an agent[21] or a LET provider may use an agent.. Or both could use a common third party to undertake or support part of the activities or processes associated with a learning transaction.

Note: Addressing the roles of “agents” and “third parties” in a learning transaction with respect to privacy protection of personal information could be standards development work undertaken as a new Part of ISO/IEC 29187.

[20] On the role of “an “agent” and the role of a “third party”, as well as the need to maintain a clear distinction between the two, see Clause 6.2.5 “*Person and delegation to “agent” and/or “third party”* in ISO/IEC 15944-1:2010.

[21] For example, an individual who is mute may use an agent to assist in communications (e.g., someone who “signs” = use sign language). An example of a LET provider using an agent could be contracting out a particular aspect of its activities.

9. What is the generic approach to management of identities of an individual?

9.1 During its lifetime, an individual has many differing personae. Some of these are assigned to him/her, (e.g. birth name, Latin-1 character name on a passport, etc.). Others are those by which the individual wishes to be known and thus identified by (e.g., common use daily name, married name, internet e-mail address name, social networking persona, etc.). In addition, the original persona may consist of such a numerous set of characters (e.g. surname) that it is too long to "fit" on documents (e.g. passports) and identification cards[22] (of all kinds and for varied purposes). Thus the persona needs to be shortened, i.e. "truncated". This is known as a "truncated name" and "truncated recognized name" (TRN).

A "persona" is defined in ISO standards as,

ISO/IEC 15944-1:2002 (3.51)	persona	99	set of **data elements** and their values by which a **Person** wishes to be known and thus identified in a **business transaction**	persona	01	série d'**éléments de données** et leurs valeurs selon lesquelles une **Personne** désire être connue et ainsi identifiée dans une **transaction d'affaires**

Not all the personae used by a Person are "legally recognized", i.e. are of the nature of a "legally recognized name (LRN)". The same applies to the personae of an individual, i.e., as a "recognized individual name" (RIN).

Further, at any point in time of its life, an individual may well have, and often has more, than one "RIN" (especially for those who migrate to another county, get married, whose birth name is written use non-Latin characters, etc.).

The same is thus also true in a LET environment and the RINs and other persona of an individual learner, as well as the LRN(s) of a LET provider.

The ISO definitions for "legally recognized name" and "recognized individual name" are as follows:

ISO/IEC 15944-5:2008 (3.72)	legally recognized name (LRN)	99	**persona** associated with a **role** of a **Person** recognized as having legal status and so recognized in a **jurisdictional domain** as accepted or assigned in compliance with the **rules** applicable of that **jurisdictional domain**, i.e. as governing the **coded domain** of which the **LRN** is a member NOTE 1 A LRN may be of a general nature and thus be available for general use in	nom légalement reconnu (NLR)	01	**persona** associée au **rôle** d'une **Personne** reconnue comme ayant un statut légal et ainsi reconnue dans un **domaine juridictionnel** comme acceptée ou attribuée conformément aux **règles** applicables de ce **domaine juridictionnel**, c.-à.-d. celles régissant le **domaine codé** dont le **NLR** est membre NOTE 1 Un NLR peut être de nature générale et ainsi être disponible pour usage général dans l'échange d'engagements ou peut découler de l'application d'une loi, d'un règlement, d'un programme ou d'un

[22] The standard default maximum number of characters on an "embossed" credit or debit card is 35 characters.

			commitment exchange or may arise from the application of a particular law, regulation, program or service of a jurisdictional domain and thus will have a specified use in commitment exchange. NOTE 2 The process of establishment of a LRN is usually accompanied by the assignment of a unique identifier. NOTE 3 A LRN is usually a registry entry in a register established by the jurisdictional domain (usually by a specified public administration within that jurisdictional domain) for the purpose of applying the applicable rules and registering and recording LRNs (and possible accompanying unique identifiers accordingly). NOTE 4 A Person may have more than one LRN (and associated LRN identifier).			service particulier d'un domaine juridictionnel et ainsi avoir un usage spécifié dans l'échange d'engagements. NOTE 2 Ce processus d'établissement d'un NLR s'accompagne habituellement de l'attribution d'un identificateur unique. NOTE 3 Un NLR est habituellement une entrée de registre dans un registre établi par le domaine juridique (habituellement par une administration publique spécifiée dans ce domaine juridictionnel) aux fins d'application des règles applicables et de l'enregistrement et de l'inscription des NLR (et par conséquent de leurs identificateurs uniques possibles les accompagnant). NOTE 4 Une Personne peut avoir plus d'un NLR (et identificateur NLR connexe).

ISO/IEC 15944-5:2008 (3.114)	recogni-zed individu al name (RIN)	99	**persona** of an **individual** having the properties of a **legally recognized name** (**LRN**) NOTE 1 On the whole, a persona presented by an individual should have a basis in law (or recognized jurisdictional domain) in order to be considered as the basis for a recognized individual name (RIN). NOTE 2 An individual may have more than one RIN and more than one RIN at the same time. NOTE 3 The establishment of a RIN is usually accompanied by the assignment of a unique identifier, i.e. by the jurisdictional domain (or public administration) which recognizes the persona as a RIN.	nom reconnu d'individ u (NRI)	01	**persona** d'un **individu** ayant les propriétés d'un **nom reconnu légalement (LRN)** NOTE 1 En définitive, une persona présentée par un individu doit avoir une base légale (ou un domaine juridictionnel reconnu) pour être considérée comme base d'un nom reconnu d'individu (NRI). NOTE 2 Un individu peut avoir plus d'un NRI ou plus d'un nom reconnu d'individu en même temps. NOTE 3 L'établissement d'un nom individuel reconnu s'accompagne généralement de l'attribution d'un identificateur unique par le domaine juridictionnel (ou l'administration publique) qui reconnaît la persona comme nom reconnu d'individu (NRI).

Depending on the roles which a Person qualifies for, a Person will be assigned an identifier, a member of a that “club”, by a Source Authority as”. The Source Authority here is the Person responsible for the operation of the Registration Schema which assigns identifiers to Persons who qualify to become members of that “club”. The metaphor of “Club” is used here for any organization or public administration which operates an identification schema based on an “identification” process, the result of which is the assignment of an “identifier” to a qualifying entity.

In the context of a business transaction (including a learning transaction), the fact that a goal has been defined to and the commitment agreed usually includes the signatures of the participating Persons, i.e. a “Person signature”.

The ISO definitions for “identification”, “identifier” and “Person signature” are:

ISO/IEC 15944-1:2002 (3.26)	identification	99	**rule**-based **process**, explicitly stated, involving the use of one or more **attributes**, i.e., **data elements**, whose value (or combination of values) are used to identify uniquely the occurrence or existence of a specified **entity**	identification	02	**processus** basé sur des **règles**, énoncées explicitement, impliquant l'utilisation d'un ou plusieurs **attributs**, c.-à-d. des **éléments de données**, dont la valeur (ou une combinaison de valeurs) sert à identifier de façon unique l'occurrence ou l'existence d'une **entité** spécifiée

ISO/IEC 15944-1:2002 (3.27)	identifier (in business transaction)	99	**unambiguous**, unique and a linguistically neutral value, resulting from the application of a **rule**-based **identification process** NOTE 1 Identifiers must be unique within the identification scheme of the issuing authority. NOTE 2 An identifier is a linguistically independent sequence of characters capable of uniquely and permanently identifying that with which it is associated. {See ISO 19135:2005 (4.1.5)}	identificateur (transaction d'affaires)	01	valeur **non-ambiguë** et linguistiquement neutre, résultant de l'application d'un **processus** d'**identification** à base de **règles** NOTE 1 Les identificateurs doivent être uniques dans le système d'identification de l'autorité émettrice. NOTE 2 Un identificateur est une séquence de caractères linguistiquement indépendante capable d’identifier de façon unique et permanente ce à quoi il est associé. {voir ISO 19135:2005 (4.1.5)}

ISO/IEC 15944-1:2002 (3.50)	Person signature	99	signature, i.e., a **name** representation, distinguishing mark or usual mark, which is created by and pertains to a **Person**	signature d'une Personne	01	signature, c.-à-d. la représentation d'un **nom**, marque de distinction ou marque habituelle, qui est créée par une **Personne** et se rapporte à celle-ci

The use of various combinations of personae, identifiers and signatures by an individual in a business transaction (or individual learner in a learning transaction) is summarized in the following Figure J, which is an adaptation of Figure 11 in ISO/IEC 15944-1 and Figure 6 in ISO/IEC FDIS 15944-8.

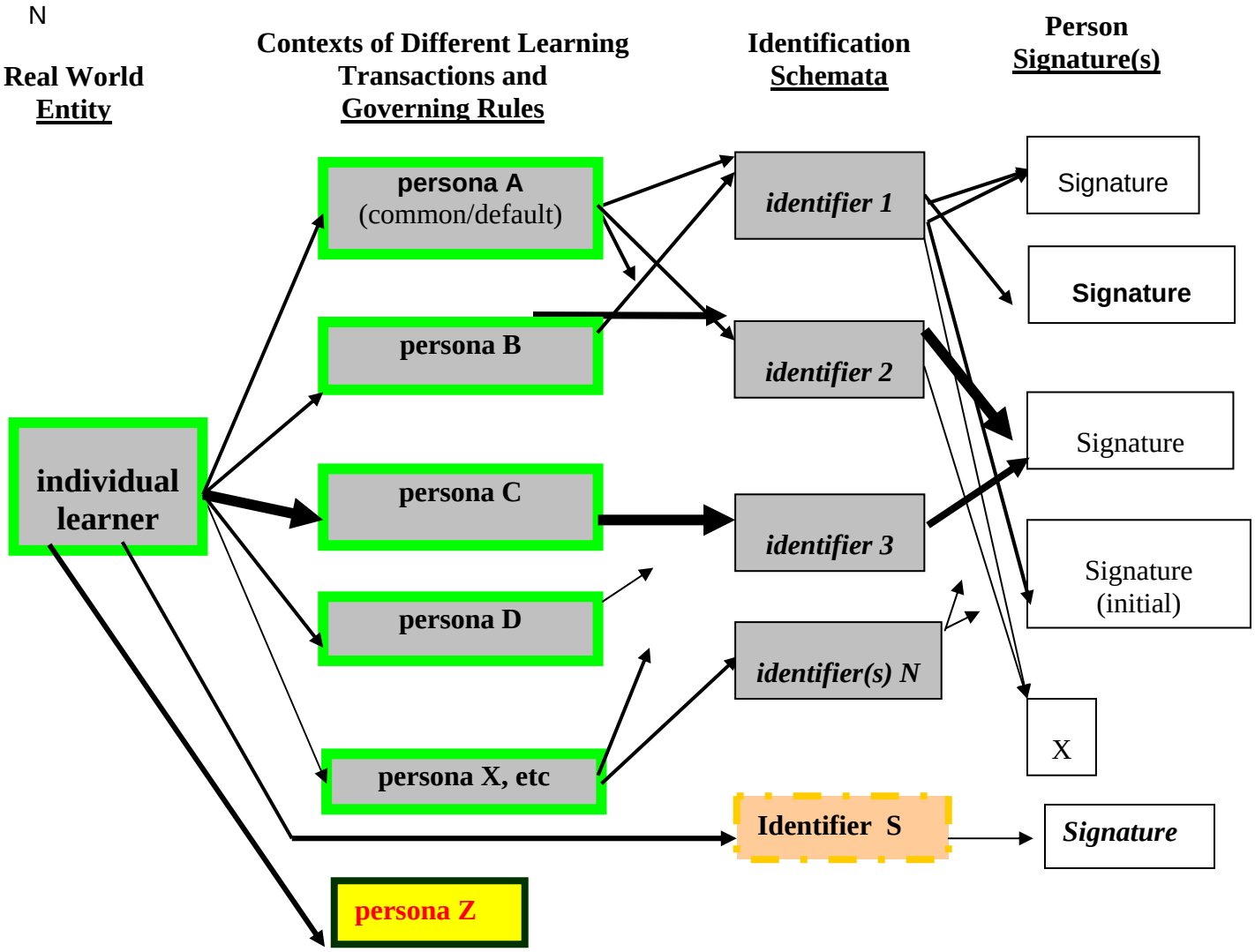


Figure J — Illustration of relationships of links of a (real world) individual to (its) persona (e) to identification schemas and resulting identifiers to associated Person signatures[23] — in the context of different learning transactions and governing rules

Based on the above figures which summarizes a whole set of rules is evident that an individual can have many different and distinct "individual identities". Figure I is an adaptation of a generic model. In a LET and privacy protection context, the focus here is on the individual as a learner, .i.e. as an individual learner. Figure I is an adaptation of the generic model. An "individual identity" in turn is a sub-type of "Person identity" whose ISO definition is:

ISO/IEC	Person	99	combination of **persona information**	identité d'une	01	combinaison de l'**information** d'une

[23] Use of different forms in the boxes for "signature" reflects the fact that a Person can have more than one and different signature forms and representations (in hard copy or digital form).

15944-1:2002 (3.49)	identity (Pi)		and **identifier** used by a **Person** in a **learning transaction**	Personne (Pi)		**persona** et de l'**identificateur** utilisé par une **Personne** dans une **transaction d'affaires**

In addition the ISO definition for "individual identity" is:

individual identity (ii)
Person identity *of an* ***individual****, i.e. an individual identity, consisting of the combination of the* ***persona*** *information and* ***identifier*** *used by an* ***individual*** *in a* ***business transaction****, i.e. the making of any kind of* ***commitment***

The following figure, K (also extracted from ISO/IEC 15944-1 & ISO/IEC FDIS 15944-8) demonstrates this.
N

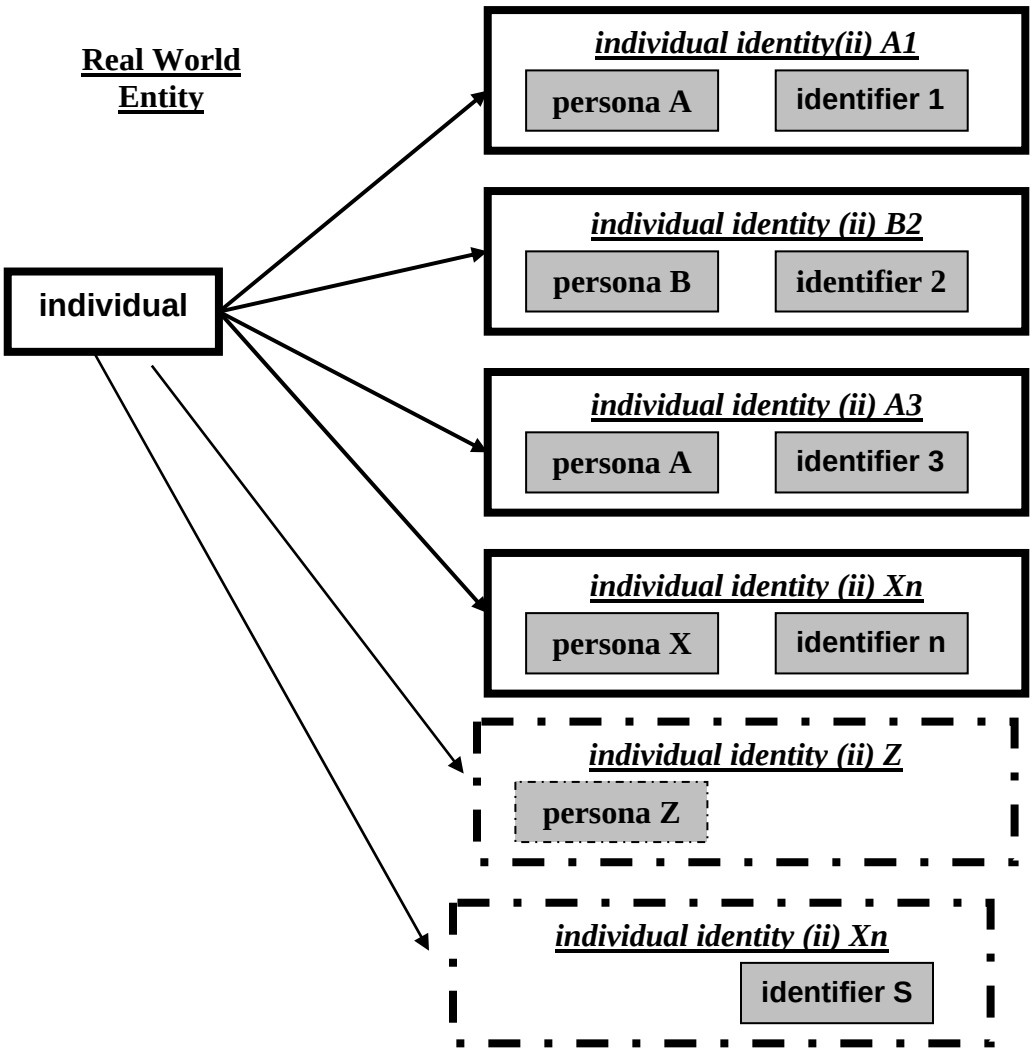


Figure K — Illustration of range of links between personae and identifiers of an individual identity (ies) of an individual

Finally, under this topic is the matter of recognition of an individual identity. Here one must take into account that an individual may have several "recognized individual identities (RIIs)". A recognized individual identity established in one context may not be acceptable in another context. There are two basic options for establishment and use of a recognized individual identity. These are illustrated in the figure L below, also extracted from ISO/IEC FDIS 15944-8.
n

.

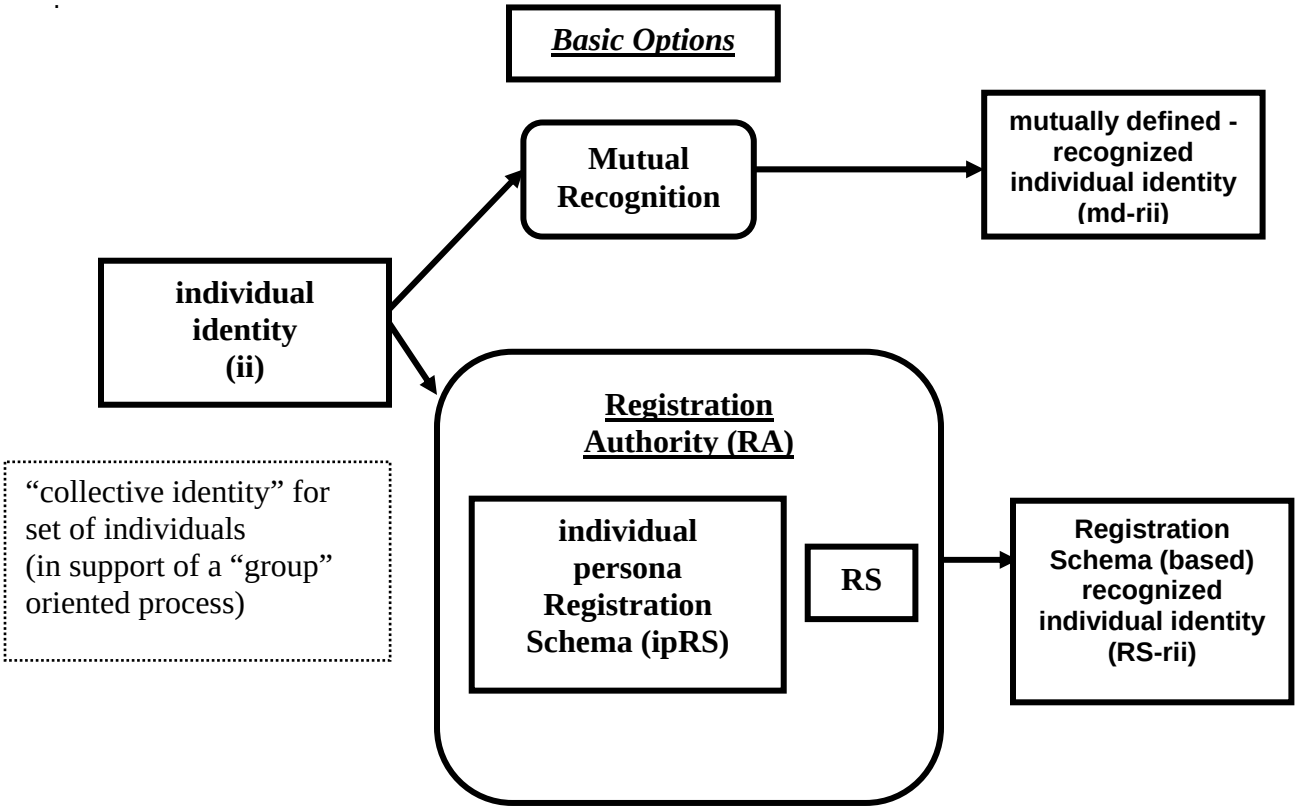


Figure L — Illustration of two basic options for establishment of a recognized individual identity (rii)

One concludes that the use of a common reference of Registration Authority is the more common and efficient approach.

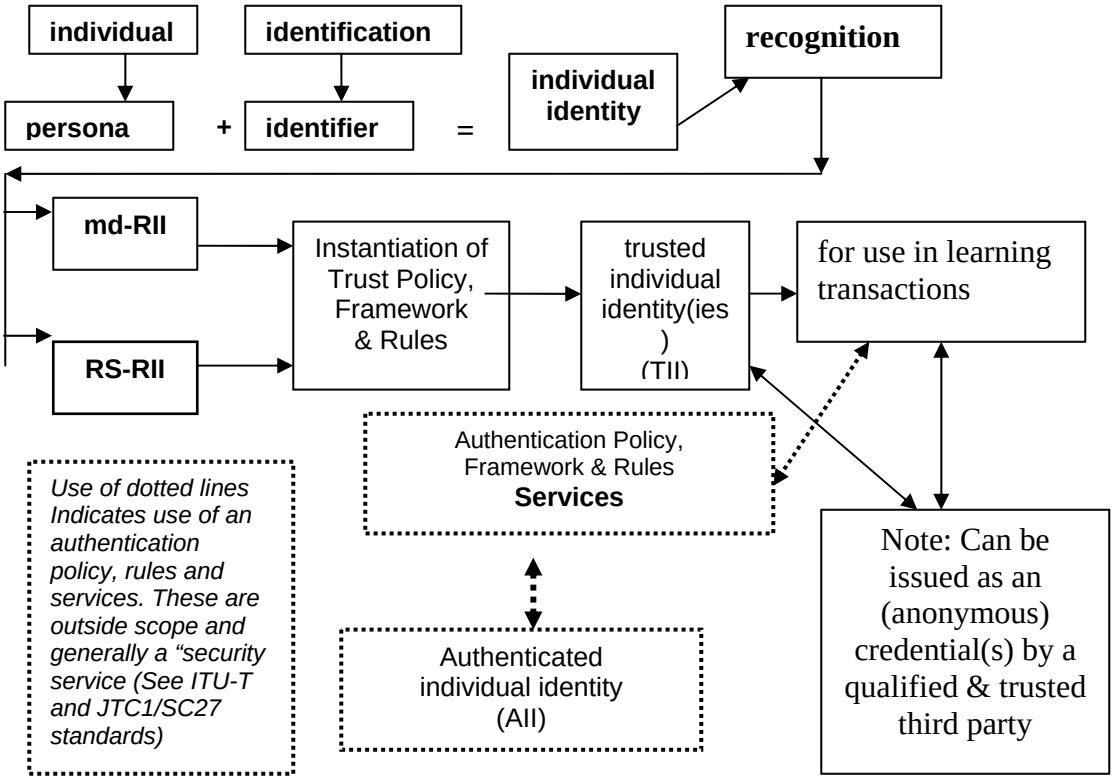
It is noted that one has established a "recognized individual identity"(RII), the next question is whether or not that RII can be **trusted** for use with respect to the goal of the learning transaction.[24] This is an individual learner will have more than one RII. Which of these, if any, can be trusted to be fit for purpose for authentication the individual identity as (part of the trust framework for management of identities with respect to the learning transaction (or class of learning transactions)? This is illustrated in the following figure K.

[24] This text and figure K has been added on Monday, 26 June, 2010 as a partial response, link to the issuance by the US government on 25 June of a document titled " *Draft – National Strategy for Trusted Identities in Cyberspace; Creating Options for Enhanced Online Security and Privacy"*, See further,

< http://whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace >

n

Figure K: Illustration of Implementation of the US Draft "National Strategy for Trusted Identities in Cyberspace" (based on ISO/IEC 15944-1, 15944-8 and under development new ISO/IEC21987-1 Privacy protection in LET Part 1: Framework Model)



n

10. What are the "security services" aspects of privacy protection requirements?

For some reason, discussions on and development of standards in support of privacy protection in the ISO/IEC JTC1 Information technology community seem to be dominated by an approach which views such standards development as being primarily of a "security techniques" nature[25].

Here one notes that other ISO standards development committees have been successful in developing standards supporting compliance with privacy protection requirements in their sectors without such a heavy emphasis on "security services and techniques". These include[26]:

- ISO TC 68 – Financial Services
- ISO TC 204 – Intelligent Transportation Systems
- ISO TC 215 – Health informatics
- ISO/IEC JTC1/SC32 – Data Management and Interchange

Further one notes that of the 11 common Privacy Principles identified above, only one deals with matters of a "security techniques and services" nature, i.e., Principle 8: Safeguards.

A major study commissioned by International Conference of Privacy and Data Protection Commissioners in 2004 undertaken in the context of "PETTEP"[27] identified seventeen (17) "Privacy Threads" and classified them into three categories namely, accountability, data management and security as follows:

- accountability threads

    1. accountability
    2. challenging compliance
    3. openness
    4. individual access
    5. accuracy

- data management threads

    6. unlinkability
    7. unobservability
    8. pseudonymity
    9. anonymity
    10. deletion
    11. consent

[25] See further the work of ISO/IEC JTC1/SC27 IT security Techniques and in particular its WG5 "Identity management and privacy technologies".

[26] The ISO committees and their standards relevant to privacy protection were identified by the ISO/IEC JTC1/SC36 Ad-Hoc on Privacy and so reported as part of document JTC1/SC36 N1737 which was the New Work Item Proposal (NWIP) serving as the rationale and business case for the start of the this ISO/IEC 29187 "ITLET & Privacy protection standards project.

[27] PETTEP = Privacy Enhancing Technology Testing and Evaluation Project

12. identifying purpose
13. limit use/disclosure
14. non-collection
15. limit collection
16. data scarcity

- security threads

17. security and safeguards

Finally, from an “ITLET and Privacy Protection” standards development perspective and based on user requirements identified via the JTC1/SC36 Ad-Hoc on Privacy, the priority of standards development work for ISO/IEC 29187 is in support of the “Learning Operational View” perspective.

Annex A – List of ISO/IEC Standards Referenced

The complete titles of the standards referenced in this document are presented below. Some are available in both ISO English & ISO French [28] ether via separate documents (= E+F) of in a single English/French side-by-side document (= E/F). In some cases, the standards listed below are available in "ISO English" only but their Clause 3 Definitions are available in both ISO English & ISO French (and possibly other languages as well). Where this is the case, this is noted as "E/F definitions" or if more than E/F as "E/F+ definitions". Many of these standards have been made freely available by ISO. A key reason here is that they serve as base standards and serve as key "foundation" building blocks in the development of other standards. This is indicated by an "*" in front of the entry for the standard. URL where these standards can be found for download is http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

* ISO/IEC 2386-36:2009 Information technology — Vocabulary — Part 36: Learning, Education, and Training / Technologie de l'information — Vocabulaire — Partie 36: Apprentissage, éducation et formation (E/F)

* ISO/IEC 14662:2010 Information technology — Open-edi reference model /Technologies de l'information — Modèle de référence EDI-ouvert (E/F), 3rd ed.

* ISO/IEC 15944-1:2010 *Information technology — Business agreement semantic descriptive techniques — Part 1: Operational aspects of Open-edi for implementation Technologies de l'information — Techniques descriptives sémantiques des accords d'affaires — Partie 1: Aspects opérationnels de l'Edi ouvert pour application* (E) + (E/F definitions), 2nd ed.

* ISO/IEC 15944-5:2008 Information *technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints Technologies de l'information — Vue opérationnelle d'affaires — Partie 5: Identification et référence des exigences de domaines juridictionnels en tant que sources de contraintes externes* (E) + (E/F definitions).

* ISO/IEC 15944-7 :2009 Information technology — Business Operational View — Part 7: eBusiness vocabulary / Technologies de l'information — Vue opérationnelle d'affaires — Partie 7: Vocabulaire e-affaires (E) +(E/F+ definitions)

* ISO/IEC FDIS 15944-8:2010 *Information technology - Business operational view Part 8: Identification of privacy requirements as external constraints on business* (E) + (E/F definitions).

[28] The use of "ISO English" and "ISO French" refers to the use of the English and French languages in ISO standards. This recognizes that many countries across the world use these languages with different forms of spelling and/or choice of words for the same entity.

Annex B - ABSTRACT

The legal requirement of “data protection”, introduced in Europe well over three decades ago, focussed on “machine-readable records”, i.e. digitized recorded information only. The North American concept of “privacy”, when introduced in laws and regulations of various jurisdictional domains, applied to all forms of recorded information (including hard-copy records). The past three decades have seen major changes in information and communication technologies (ICT) and these will continue to evolve and morph. The introduction and widespread use of the Internet, since the mid-1990`s with its direct access and use by individuals as well as the recent advent of `social networks” has demonstrated that a technology-based approach to privacy protection has major drawback, i.e., by the time it is developed and implemented the technologies have changed, morphed, and new ICTs introduced..

On the other hand, privacy protection requirements pertaining to personal information on or about an identifiable individual are quite stable and likely will remain so in the future. The challenge is one of bridging the real world of privacy protection requirements as a right of an individual in the dematerialized world of the Internet. This is possible if one takes an IT-platform neutral approach. The purpose of this public lecture is to demonstrate the viability and practicality of such an approach.

Based on existing international ISO standards (made publicly and freely available by ISO as they are “foundation” e-Business standards), this lecture will bring forward key issues which already have been resolved in an IT-neutral but IT-enabled manner bridging both legal requirements and an ICT environment, including

- What are the common eleven (11) principles governing privacy protection (based on the OECD Guidelines, EU Directives & APEC Framework)?
- Need for an IT-platform Neutral Approach
- Importance and role of concepts, their definitions and associated terms
- What is a `”Person`”? and its subtypes of “individual”, “organization” & “public administration”?
- What is “recorded information”? and what is “personal information`”
- What are the key public policy requirements impacting use of ICT as rights of an individual of which privacy protection is part?
- Why should privacy protection be viewed and modelled from a “(learning) transaction” and “collaboration space” perspective?
- What are the common eleven (11) principles governing privacy protection (based on the OECD Guidelines, EU Directives & APEC Framework)?
- What is the generic approach to management of identities of an individual?
- What are the “security services aspects” of privacy protection requirements?

Note: Since the focus of this lecture is that of privacy protection in a LET context and is based on existing ISO standards and standards development work, there will be a handout listing all ISO documents referenced as well as those of JTC1/SC36 ITLET.

Annex C - Resumé for Dr. Jake V. Th. Knoppers

(tel: +1-613-234-3244; fax: +1-613-234-3935; e-mail: mpereira@istar.ca)

(Prepared for the context of the AFNOR Workshop "ITLET and Privacy Protection Standards Development", Paris, France, 28 June-2 July, 2010)

Currently President of Canaglobe™ International Inc., and Senior Vice-President of Information Management Services (INFOMAN®) Inc., Dr. Knoppers has over twenty years experience in strategic planning, policy development, (e.g., privacy, security, access-to-information, copyright), transborder data flows, data abuse and computer crime, admissibility of computer-generated records, etc.), information (life cycle) management, product positioning and marketing, and done so from a user perspective. He has served as a senior advisor to key public sector agencies and private sector companies as well as joint public/private sector task forces in the areas noted above. Through the years, he has developed extensive experience and expertise in standards development nationally and internationally in the various fields related to information management (IM) and information technology (IT) including e-commerce, e-business, e-government, e-geomatics, e-trade, e-metadata, etc. His various activities currently include serving as the Senior Advisor to the Canadian eCommerce Standards Strategy Team a joint public/private sector initiative.

Dr. Knoppers assisted in the development of The Canadian Electronic Commerce Strategy and was Head of the Canadian delegation to the earlier ISO/IEC JTC1 "Business Team on Electronic Commerce". He is a member of the Technical Committee on Information Technology (TCIT) of the Standards Council of Canada, which coordinates Canadian contributions and positions in international standards development work with respect to information and communications technologies (ICT) including that pertaining to e-business/e-commerce. Dr. Knoppers is Vice-Chair of the Canadian Advisory Committee (CAC) for ISO/IEC JTC1/SC32 `"*Data Management & Interchange*`` and Chair of the CAC for ISO/IEC JTC1/SC36 "*Information technology for Learning, Education and Training*" (ITLET).

In the area of international standards development, he is the Project Editor or Co-Project Editor for three JTC1/SC32 standards and three JTC1/SC36 standards including with Renaud Fabre (France) the ISO/IEC 29187 *Information technology – Identification of privacy protection requirements pertaining to Learning, Education and Training (LET* ", and in particular the development of ISO/*IEC 29187-1 – Part 1: Framework Model"*

The focus of effort of the standardization work of Dr.Knoppers is that of the "WHATs" not the "HOWs" doing so from a user operational requirements view perspective (including legal requirements) with an emphasis and focus on portability, interoperability, IT-enablement, cultural adaptability and re-usability.

An economist by training, Dr. Knoppers received his Ph.D. (cum laude) from McGill University, Montreal and as a Killam Fellow undertook advanced multidisciplinary post-doctoral research in economics, history, international trade, computer science and long term structural changes. He has numerous publications in these areas as well as in information policy, information management and, more recently, standardization and e-business.

- - - - -