Privacy

At its plenary in May 2015 COPOLCO decided to request the WGGM to undertake a gap analysis of existing standards within ISO, IEC and ISO/IEC JTC1, the ITU and UN/ECE on privacy and protection of personal data in order to identify areas needing further work in consumer protection, for the consideration of the COPOLCO Chair's Group at its meeting in November 2015.

The WG requested Mr Peter Eisenegger, a presenter at the 2015 COPOLCO workshop, on the topic of privacy from a consumer viewpoint, to undertake this task.

Mr Eisenegger's expert view, with which the WG Chair agrees, was that given the scale and scope of the privacy challenges, further gap analysis work by COPOLCO alone would take too long and it would be difficult on a voluntary basis to find the necessary expertise across all the ICT areas involved. It was agreed that a more strategic approach could get a better result.

Because it was not realistic to make an exhaustive inventory, i.e. a classic gap analysis, Mr. Eisenegger developed an overall strategic identification of the issues and observations about the extent (or lack) of what standards are currently covering is where it could be useful. The COPOLCO Chair's Group commented on a first draft of the first "gap analysis" which was a good start, and invited some volunteers to assist and comment on its further development of it from the consumer perspective.

As a key spin off from this gap analysis work Mr Eisenegger produced a list of consumer privacy needs and identified those needs that are relevant to a number of categories, specifically: consumer digitally connected devices as part of the Internet of Things (which includes smart phones, home appliances, wearables, cars and more), Smart Cities, Social Media and Big Data.

The Chair of the WGGM, the COPOLCO Secretariat and Pete Eisenegger had a WebEx link-up on 20 February 2016 to discuss the way forward on the Privacy matter given Mr Eisenegger's time constraints. The following was the agreed outcome of the discussion.

1. **Contact with COPOLCO:** Mr Eisenegger will be the main contact point on privacy for COPOLCO, interacting primarily with the COPOLCO WGGM.

2. **Privacy group and networking:** Mr Eisenegger volunteered to provide "thought leadership". He would prefer to engage an informal group of volunteers composed of consumer representatives on JTC1 identified from the Global Directory, in a forum modelled after ANEC's working methods, working mostly by e-mail. The COPOLCO Secretary and Mr Eisenegger are working together to set up a suitable group for exchange of ideas and information among consumer representatives potentially interested in privacy issues (e.g. experts participating in JTC1 working groups who are identified in the Global Directory as consumer stakeholders, and potentially others). When formed, Mr Eisenegger will approach the GD experts as the pool for the network. Mr Eisenegger will share his materials on the Internet of Things, including the slide set from the May 2015 COPOLCO workshop, with interested consumer representatives.

   Mr Eisenegger proposed that as a priority COPOLCO should coordinate ICT consumer reps on the ISO data base

3. **Representation:** in his ICT Consumer Coordinator role and member of BSI ITC 1 mirroring JTC1, , Mr Eisenegger supported the COPOLCO resolution for improved consumer representation with respect to ICT standards and has also worked with the COPOLCO Secretary and Chair of the WGGM towards this goal. BSI ICT 1 made him a UK delegate to the March meeting of the JTC 1 Joint Advisory Group (JAG). For the time being he is working towards becoming a standing member of JTC 1 JAG group as in order to provide a consumer viewpoint on issues in JTC1 and with a particular focus on the data privacy space: in particular:
   a. IoT design good practices for digitally connected devices
   b. Traceability of data transfer and trading standards –
   c. Personal data processing privacy and governance - privacy good practice.

Mr Eisenegger attended the JTC1 Joint Advisory Group meeting on 15 March and brought up the issue of ongoing consumer representation. Certain concepts he introduced at that meeting, notably the cross-cutting nature of good digital practice standards, e.g. on accessibility, privacy, and vulnerability, were not widely understood by the group. The COPOLCO Secretary and Technical Group Manager will continue to investigate ways to facilitate Mr. Eisenegger's positive engagement with the JTC1 JAG. He will also prepare an issues paper for advance consideration at the next meeting (see below).

Mr Eisenegger will **develop an overall short paper for JCT 1 JAG** on consumer representation by April to mid-May. This would be a scene setter as a key backdrop to the Privacy by Design (PbD) NWIP and would address the issue of why we have selected this particular standards area of "by design" to put forward as perhaps the key consumer priority.

4. **Work with Consumers International on privacy:** Mr Eisenegger is discussing ideas on how to familiarize consumer representatives with privacy concepts through on-line and face-to-face courses. This activity is entirely self-generated and voluntary. The 3 parties involved have heavy workloads, both voluntary and commissioned. While there were hopes originally that that this mapping out these ideas could happen within 2-3 months, with Sadie Homer and Julie Hunter the current situation is significantly longer term and may slip further. Sponsorship for this work would change that situation.

5. **Privacy by design:** The WGGM Chair and Mr Eisenegger agreed to work together on a new activity template to build support within COPOLCO launching a New Work Item Proposal on privacy by design standards. The aim is to reduce risks, and generic standards do not currently go far enough. Work on this will begin Mid May and needs to understand and assimilate any of the relevant work within JTC1 produced recently, for example on Privacy Engineering and IoT use cases.

6. **Key person:** Mr Eisenegger confirmed his willingness to be COPOLCO's key person on privacy, but limit this activity to a report of activity to go into the annual Consumers and standards update report and answer questions from experts on privacy issues.

7. **Gap analysis:** The WGGM Chair and the COPOLCO secretary have finalized the "gap analysis" report with input from volunteers in the Chair's Group and with the final OK from Mr Eisenegger (See the annex). Alongside the privacy guides Mr. Eisenegger mentioned at the 2015 COPOLCO workshop in May 2015, this will be a good resource and briefing paper for COPOLCO and privacy network experts.

Action at Fringe meeting: decide on action plan on Privacy for the next 12 months.

Identification of current consumer issues in privacy and protection of personal data
Report to COPOLCO, based on a preliminary report to the Chair's Group

---

Peter Eisenegger, COPOLCO Key Person Data Protection and Privacy

1. Introduction

Commissioning this report

In Geneva May 2015 COPOLCO resolved to undertake a privacy needs gap analysis as in the COPOLCO resolution below.

COPOLCO Resolution 8/2015
2015 workshop, The connected consumer in 2020 – empowerment through standards
"decides to request the Consumer protection in the global marketplace working group to undertake a gap analysis of existing standards within ISO, IEC and ISO/IEC JTC1, the ITU and UN/ECE on privacy and protection of personal data in order to identify areas needing further work in consumer protection, for the consideration of the COPOLCO Chair's Group at its next meeting in November 2015,"

At COPOLCO's request Peter Eisenegger, as COPOLCO's key person for data protection and privacy, has under taken a preliminary gap analysis, drawing largely on a study of Smart Cities and JTC 1 SC 27 WG 5, IT *Security Techniques* and produced this report for COPOLCO. The review and its report is a first step in the COPOLCO process of identifying and confirming gaps in current international standards addressing consumer/citizen privacy needs. One challenge met in this report has been how to review, on a voluntary basis, such a large set of technical standards and reports relevant to consumer privacy.

2. The Privacy approach taken in this review:

2.1. Privacy standards – generic or specific?

The starting point for the review is the COPOLCO detailed list of privacy needs, provided in Annex 1. These needs are based on BSI/CPIN and ANEC Privacy Guides for consumer representatives. These guides cover the developed countries' privacy needs and COPOLCO representatives for developing countries are currently examining whether any extra needs and requirements should be added from their perspective.

The approach adopted for this report is that privacy needs are best addressed in a manner that is more like product safety implying that product and service specific standards are required.

Of the privacy initiatives under way, that of the EU's Privacy by Design (PbD) M530 standards development programme is on track to achieve better products and service specific standards by developing good practice for privacy by design for products and services.

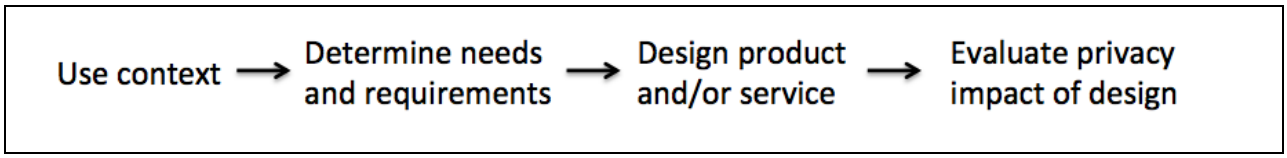
For this report, only ISO standards and working documents have been readily available, and time and effort constraints have only allowed a few of those to be reviewed. The author has

already reviewed some documents referenced in the report at an earlier date in order to contribute to UK National Body reviews and formal National Body comments.

2.2. Privacy by Design (PbD)

In overview a PbD approach needs generic standards for the design and design updating process with “use cases” providing the context for which privacy has to be designed in. Figure 1 provides a simplified PbD process flow.

Figure 1 A simplified Privacy by Design process



Standards are needed that ensure that the right use context is set for determining which privacy needs and requirements have to be met by the designers. Then once a design is mature enough to be evaluated a privacy impact assessment process is run and from that an impact statement or measurement is determined that leads to a go/no go decision on the design.

However the design and implementation issues run deeper than that, as designs and their real life implementations have to be kept under review and assessed for their privacy impact throughout the product or service lifecycle. A case in point is the CEN TC 225 Liaison report for CEN/CENELEC JWG 8 in which the prior EU state of the art work on RFID privacy impact assessment was reviewed (the report is available upon request).

3. Taking Privacy by Design as an approach to meeting consumer privacy needs.

3.1. Generic standards

The EU’s M530 programme is likely to deliver a great deal that is relevant, however that EU work itself will be founded on ISO/IEC JTC 1 generic standards and so a key part of this review has looked at the privacy needs gaps issues in the JTC 1 domain in as much detail as possible with voluntary effort. However when it comes to product and service use case specifics then JTC 1, while having sub committees pertaining to some sectors, is nonetheless very generic in its standards requirements.

3.2. Context and use standards

While much of JTC 1’s work is generic, it is possible to find this type of context and use approach within ISO/IEC JTC 1. For example, Big Data has a proposal for both use cases and utilizing templates to provide context. At the end of August 2015 the ISO/IEC JCT1/WG9 on Big Data issued a contribution on Big Data Use Cases and Derived Requirements, ISO/IEC JCT1/WG9 N103. This document itself builds on the ISO/IEC Cloud Computing SC38 Standing Document 2 which gives the compendium of Cloud Computing Usage Scenarios and Use cases, as well the associated methodology and guidelines.

This might mean that the wider ISO Technical Committee community have to be involved for product and service specifics. Annex 2 provides an analysis of the coordination and involvement that might be involved for COPOLCO and the Technical ISO Management Board to consider.

Then beyond ISO's own TC's there are even wider issues of liaison and coordination with a significant number of other international standards bodies such as the ITU, ETSI and others.

4. Summary Results of the preliminary gap analysis

The privacy needs of Annex 1, when examined in detail against the specific documents referenced in this report broadly indicated that there are three key areas where current ISO standards development seems to have significant privacy gaps that should be addressed. That said, it is important to recognise and understand that the core standards laid down by JTC 1's committees are of good quality from the consumer perspective and the issue is about building on and enhancing these where 21st Century digital privacy needs are yet to be fulfilled.

The three key strategic gaps that have been identified are illustrated in figure 2, below. They relate to protecting consumer's privacy in the domestic environment and providing privacy control, the issues of anonymity and residual identifiability and the traceability / transparency of data sharing and trading.

Gap A Domestic environment and processing: domestic privacy.

- As consumers are non-experts, domestic equipment (e.g. home, car and personal networks and devices) needs to have security controls and updating processes that are extremely easy to understand and operate.
- With frequent and/or continuous data collection, real time privacy control is needed (24/7 privacy preferences control, including in consumer-targeted software).

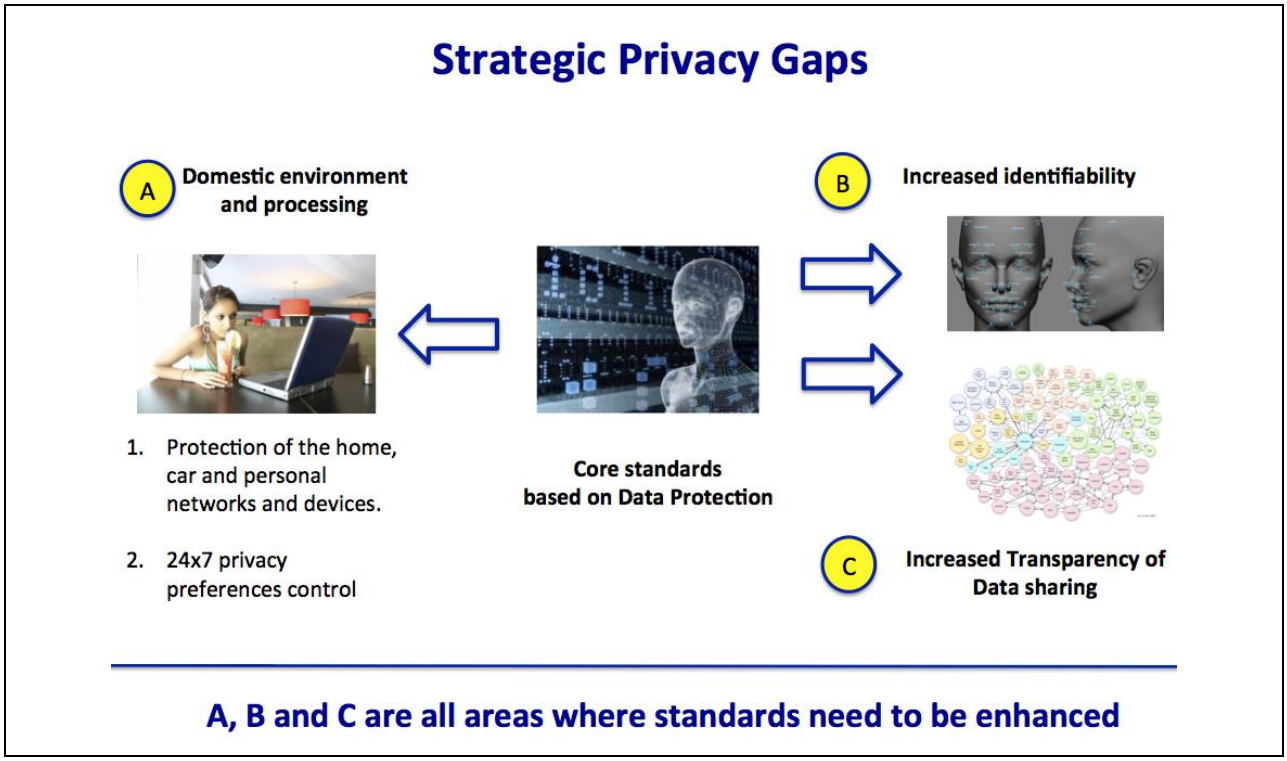
Gap B Increased identifiability: analysis of consumer data.

- Large scale data collection means that, even after anonymization, levels of residual identifiability need to be addressed.

Gap C. Increased transparency of data sharing: traceability and transparency

- In order to support data protection law in the world of data sharing and trading, technical standards are needed for traceability and transparency.

Figure 2 Strategic Privacy Gaps



5. Review of a key JTC 1 report

In order to address the gap analysis as well as the circumstances allowed, then the recently received JTC 1 report "SG 1 (Smart Cities) Second Phase Report Submitted to the October 2015 meeting in China" was very welcome. This report was used as the basis since Smart Cities[1] are an extremely wide privacy context and as such the topic embraces the great majority of privacy issues that consumers and citizens face.

The SG1 report has 3 aims expressed in its scope and purpose that relate to consumer privacy.

The aims listed are:

- investigate ICT standardization requirements and techniques that contribute to enhancing individual control over personal data while recognizing the benefit to society of the sharing of pertinent personal data;
- investigate ICT standardization requirements and techniques that contribute to enhancing cybersecurity in a smart city;
- explain the value of requirements for standardized risk assessment methodologies that underline the dependencies across organizations and sectors inherent to Smart Cities;

It should be noted this analysis is limited to two areas; smart cities and JTC1 SC 27 WG 5, and that the SG 1 Second Phase report references core ISO/IEC privacy standards that are also commented on in the review of the SG 1 report.

[1] *It is worth noting that BSI PAS's 181 and 182 are important sources in the SG1 analysis and Peter Eisenegger as BSI's ICT Consumer Coordinator was on the steering groups for both of these smart cities standards.*

5.1. Preliminary Review of Privacy Needs Gaps based on JTC 1 SG 1 Smart Cities Second Phase Report, ISO/IEC JTC 1 N12790

See Annex 1 for a summarized list of consumer digital privacy needs. Topic 1 potentially impacts all of the issues identified in Annex 1. References to relevant sections of Annex 1 are made in each of the other topics.

Topic	Smart Cities phase 2 report sections	Privacy gaps commentary
1. The consumer / citizen perspective is missing **'Privacy in Depth' model not addressed** Gap A (Domestic privacy)	5.1.2 Developing a Reference Framework for a smart city from an ICT perspective The JTC 1 Smart City Study Group considered that an effective contribution that JTC 1 could make to support smart cities would be to develop a Smart City Reference Framework from an ICT Perspective. It further concluded that this would best be done by developing three distinct, but linked, smart city views that relate to the areas of JTC 1 competence: • A Smart City Business Process View • A Smart City Knowledge Management View • A Smart City Engineering View Also it should be noted that 7.1.3 The role of JTC1 with respect to ICT Standards for Smart Cities states: "There are four differentiators that separate a city's use of ICT from that of other organizations[2]: 1. **Citizens at the centre**. The city largely exists for the benefit of its citizens, who by virtue of living in the city are impacted by many of the ICT and related services the city provides. There may be no practical "opt out" option for citizens and the city must provide a duty of care to all its citizens. In addition, increasingly citizens are driving many initiatives that are making	There is no Consumer / Citizens' view for Smart Cities The core viewpoint of consumers is embedded in the COPOLCO privacy needs, since the BSI/CPIN & ANEC privacy guides are built round the consumer perspective as expressed by the Privacy in Depth model. Privacy in depth puts the consumer / citizen at the centre of protection and control of his/her data. The different approaches of Privacy in Depth (PID) and Security in Depth (SID) model as used by JTC 1 SC 27 is explained below[3]. "The RFID PIA standard establishes a 'privacy in depth' (PID) model adapted from an ISO 27000 series 'security in depth' (SID) model. The difference between the two is that security in depth focuses on the organization and its core processing capabilities and the organization's ability to control both the technology and the processes, whereas the privacy in depth approach focuses on the consumer digitally connected device that is not under the control of the organization, especially when the application it not interacting with the consumer's device. And so PID needs at its core the privacy and

[2] Only one is mentioned here

[3] CEN TC 225 liaison report to the CEN/CENEC JWG 8 developing the work program for the EU's M530 Privacy by Design standards development

	the city work more smartly, by actively providing feedback to service providers in the city and by using the increasing number of applications designed to help them manage their own lives better in the city." *Reviewer's note: The Citizens at the Centre factor is not as strong a differentiator as put forward here. Many commercial services have no practical 'opt out' from the consumer's point of view and commercially much law and regulation confirms that businesses do have a reasonable duty of care whatever goods and services are sold to consumers.*	security capabilities of the digitally connected device. The two models complement each other with PID dealing better with the protection of individuals using digitally connected devices against a range of threats and SID protection of an organization's data including the personal data[4] collected or processed by an organization."
2. Data Protection and privacy expressed as a "barrier" Gaps B and C (analysis of consumer data, Traceability /transparency of data sharing)	In section **5.3** Smart City Knowledge Management View When examining sharing data the SG have identified the core privacy issues as barriers: "It may also need to reflect barriers to data interoperability. • Privacy - Conforming to human rights and data protection requirements when handling data that refers to people. • Security - Protecting data from accidental or malicious destruction, or unauthorized access. • Integrity - Avoiding data corruption as data is handled, copied, processed, and transported. • Quality - Characteristics of data such as completeness, validity, consistency, timeliness, accuracy, precision, and tolerance. It is important to understand the quality of data when considering if it can be reused for a new purpose • Provenance - The traceability of data, from collection, through	There is a risk that expressing these issues as barriers will lead to them not being properly addressed in standards. The approach taken for COPOLCO for the privacy needs gap analysis is to treat these topics as privacy by design issues for data transfer and sharing. Key privacy needs related to these issues are identified in Annex 1 with high level technical design requirements proposed for data transfer and sharing solutions put forward from the consumer perspective in the associated privacy guides. *Ref* *http://www.anec.eu/attachments/ANEC-ICT-2015-G-040.pdf*

[4] *defined by ISO as personally identifiable information (PII)*

	each transformation, analyses and interpretation."	
3. Consumer sourced data **A) The role in ICT systems of social media** Gaps A and C (Domestic privacy, Traceability /transparency of data sharing) **B) Data capture from sensors**	5.4 Smart City Engineering View 5.4.1 Objectives and approach The report in Figure 5.3-2 (below this table) provides an initial Smart Cities Solution Concept Diagram of an overview of smart cities organizational layers. *Reviewer's note: This picture does not include smart cities' use of consumer/citizens public and socially shared information and views. Sensor Data collected from consumer's own devices is included however as 'crowd sourced' data.*	A) In the UK BSI smart city standards work, (as well as other areas like complaints handling by companies and reputational assessment systems), social media and consumer views expressed publicly are becoming vital elements of how organisations of all types interact with their consumer customers and the public in general. This gap regarding the use of social media is addressed in the privacy guide addressing domestic privacy and the privacy of digitally connected devices section 4. *Ref.* *http://www.anec.eu/attachments/ANEC-ICT-2015-G-064.pdf* B) The sensing layer at the bottom of the diagram includes both public monitoring "City sensor webs" and "Crowdsourcing" of data from personal digitally connected devices. The privacy needs associated with such collection of sensing data are also addressed in ANEC-ICT-2015-G-064.
4. Security necessary to protect privacy Gaps A and B	9. ICT standardization requirements for cybersecurity and privacy 9.1 Two linked, but distinct areas: These two issues are often considered together, because many of the most high profile failures in handing personal data have resulted from weaknesses in cybersecurity. However, for clarity, these are best dealt with separately. Privacy is first and foremost a matter of developing and following personal data protection policies and designing ICT systems to enable this. The prevention of leakage of private data due to	JTC 1 SC27 plays a pivotal role in generic security and privacy standards and ISO/IEC 27002 *Code of practice for information security management* is specifically referred to in the report. In practice when it comes to keeping data secure inside an organization's firewall (be it personal data or any other type of data), there are a great number of very good quality standards available from SC 27.

	failures of cybersecurity is best dealt with as part of the general process of controlling access to sensitive data. 9.2.3 ISO/IEC 27002 ISO/IEC 27002 *Code of practice for information security management* is an important generic standard in this area.	The JTC 1 Smart Cities report highlights 'the prevention of data leakage as the main risk, which is true, however that means that the key security trend identified in CISCO's 2014 Annual Security Report has not been addressed. (See section 2.2 of the privacy guide ANEC-ICT-2015-G-064.) The key trend is that consumer equipment and behavior is now integrated into the organization's ICT systems and the whole security attack surface has increased significantly because of that. The implication of this is that the SC 27 "27000" series of standards should be carefully reviewed to check how well they cope with consumer digitally connected devices (such as mobile phones, gaming consoles, smart televisions etc.) that are beyond the direct usage control of the organization, and how well the security on such devices can be maintained. Also see Topic 8.
5. Overall privacy framework Gaps A and B	9.3 Privacy 9.3.2 ISO/IEC 29100:2011 Privacy framework The privacy framework is intended to help organizations define their privacy safeguarding requirements related to PII within an ICT environment	The key SC 27 standard addresses, in a good quality manner, the needs of organisations in defining their requirements for meeting the data protection principles. However 29100 is not geared to the privacy aspects of domestic purposes processing undertaken by consumers, where consumers effectively have a type of data controller responsibility. Such as quasi data controller role has been referred to by Data Protection regulators like the UK ICO. This domestic processing perspective is difficult to address in 29100 and so the domestic privacy needs identified for COPOLCO in Annex 1 are aimed

		at those privacy control needs relating to the goods and services purchased and or used by consumers. The COPOLCO privacy needs approach to domestic privacy should assist privacy by design initiatives where consumer digitally connected devices are part of the processing solution.
6. Privacy impact assessment Gaps A, B and C	9.3.4 ISO/IEC 1st CD 29134 Privacy impact assessment Guidelines A privacy impact assessment (PIA) is a tool for assessing the potential impacts on privacy of a process, an information system, a programme, another initiative and a software module or a device and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. A PIA is integral to the process for privacy risk treatment. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001. A PIA is more than a tool: it is a process that should begin at the earliest possible stages of an initiative, when there are still opportunities to influence the outcome of a project and thereby ensure privacy by design. It is a process that should continue until and even after the project has been deployed. This International Standard gives guidelines for a process on privacy impact assessments and a structure and content of a PIA report.	Privacy impact assessment is fundamental to achieving good quality privacy protecting goods and services for consumers and citizens. This standard has been reviewed and commented during its development by COPOLCO's key person for Data Protection and Privacy. The standard is still 'behind the firewall' oriented and less capable or specific when consumer digital devices are part of the system being evaluated. The following 8 PIA principles for consumer digitally connected devices were put forward for consideration in drafting ISO 29134, the principles being derived from the privacy guide ANEC-ICT-2015-G-008 on privacy impact assessment for consumer digitally connected devices. i. Assessing the privacy implications of any remote ability to cause any digital device used by consumers to power up or power down ii. Assessing the privacy implications of eavesdropping radio emissions when a device is powered up and in operation iii. Assessing the privacy implications of the device and network security, and any mismatch of security configuration between device and network

		iv. The default when data types are unknown should be evaluation of the most sensitive of personal information being processed and transmitted in both directions v. The privacy implications of the sensitivity of the data types processed and collected should be evaluated vi. Assessing the privacy implications for the degree of privacy preference control available to the user vii. Assessing the privacy implications of user behaviour and their use of digital devices should be evaluated to identify privacy risks brought about by how the device is used in domestic life viii. Assessing the risk to privacy should be evaluated for personal data lost or stolen from an organization leading to the linking of that data to an individual either through - the data itself - linking to the device used by the individual The final version of this standard will need to be carefully reviewed to establish how well it addresses the privacy assessment issues of the consumer's digitally connected device.
7. Privacy and shared data Gap B:	**9.3.6 Managing privacy when data sets are shared** One privacy issue in a smart city is related to the sharing of data. An organization might want to share an anonymized data set with another agency in the city or to provide it as open data but needs to be sure that measures are in place to address the potential for private information to be inferred from that data set, should it be aggregated with data held elsewhere.	(1) This new work item to address de-identification techniques is an important step that helps address the privacy need for anonymization listed in section 3 of the COPOLCO Privacy Needs List given in Annex 1 however there are two more key needs identifies that are closely associated with this data sharing issue in that section specifically: • the need to address re-identification and the issue

	In order to tackle this issue, guidelines on anonymization and pseudonymization are being worked in SC 27 in a recent NWIP on "Privacy enhancing data de-identification techniques" which is currently under CD ballot (N15297).	of what is the acceptable level of residual identifiability for a processing purpose • The need to address large scale profiles built up of individuals especially as many data sets are assembled where such profiles become intrusive into an individual's domestic life. (2) Section 9.3.6 of the Smart Cities report does not address at all the traceability and transparency needs that support Data Protection law and principles. These are identified in section 2 of Annex 1
8. Good quality risk assessment for the domestic environment Gap A	**10.3 What is risk assessment** **….** Risk Assessment itself describes the overall process of: • risk identification; • risk analysis; and • risk evaluation [ISO Guide 73:2009, definition 3.4.1] **Risk identification** involves identifying what might happen, or what situations might exist, that might affect the achievement of the objectives of the system or organization. It includes identifying the causes and source of the risk (or hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact. It is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" and "software" events. **Risk analysis** is about developing an understanding of the risk by determining the consequences and	(1) With consumer equipment being part of many organisation's digital processing processes in the 21st Century, then how well organisations handle risk assessment and their subsequent decisions dramatically impacts both consumer digital security (and hence privacy) as well as the organisation's own security. Many of the privacy oriented standards refer to ISO/IEC 27002 whose section 6.2.1 Mobile device policy is the nearest to addressing such domestically owned or used equipment but it is currently too business equipment oriented. The involvement of domestic equipment means that both security and privacy control needs as identified in section 1 of the Privacy Needs list in Annex 1 have to be addressed too, and currently they are not. (2) ICT risk assessment is a deeply technical and complex issue as products have both generic and specific vulnerabilities

	their probabilities for identified risk events. The consequences and their probabilities are then combined to determine a level of risk. **Risk evaluation** involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk. It uses the understanding of risk obtained during risk analysis to make decisions about future actions. *Reviewer's note : for completeness a key extract from ISO/IEC 27002:2013 is included here:* Section 6.2.1 Mobile Device Policy <u>Control</u> A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. <u>Implementation guidance</u> When using mobile devices special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of mobile devices in unprotected environments. *Reviewer's note: there has very recently been proposed a new work item proposal on Privacy-specific application of ISO/IEC 27001 – Requirements*	and exploits rise and fall in the market place with a huge amount of malicious innovation to cope with. The reviewer's experience of privacy impact assessment standards for with one of the simplest of ICT technologies suggests strongly that in addition COPOLCO need to check if there are process standards for the significant area of concern that is good practice in the collection, publication and use of product and service vulnerabilities. Further, given that neither many smaller businesses nor consumers have the expertise and resources to undertake such complex risk assessments the role of automation of PIA processes should be carefully examined for possible new standards.

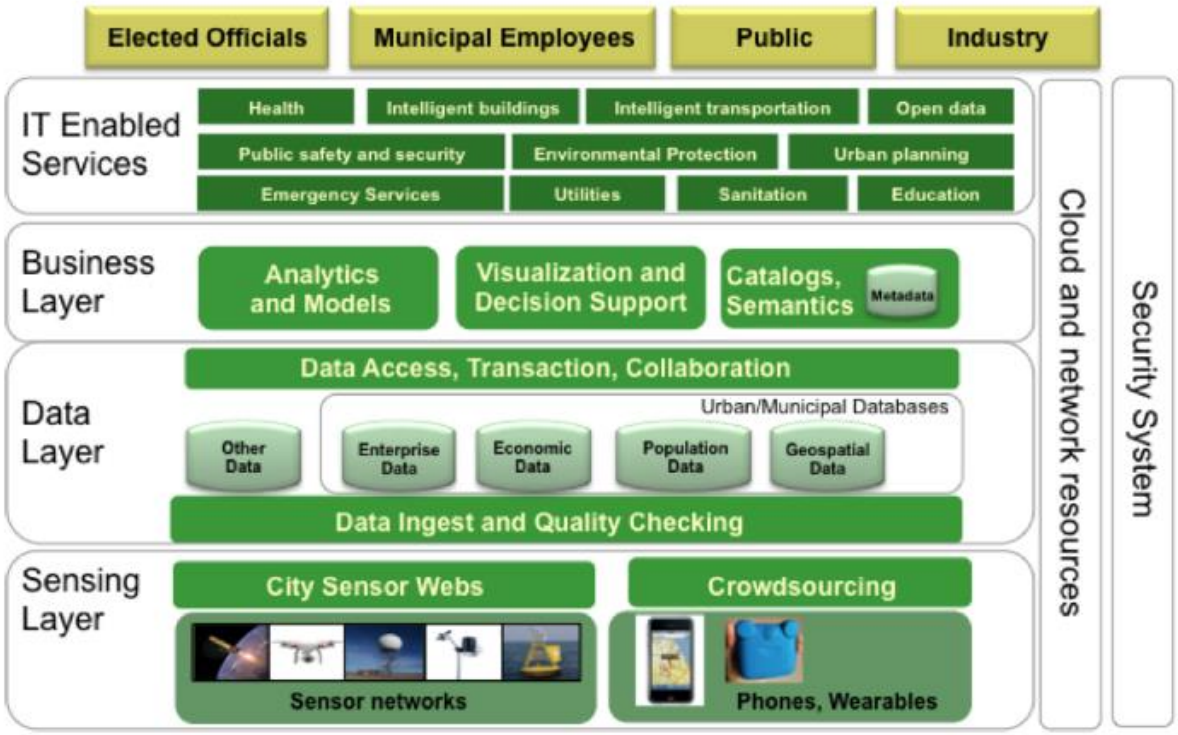


Figure 5-3 Smart Cities Solution Concept Diagram

5.2 Core JTC 1 SC27 Working Group 5 Information technology -
- Security techniques – Identity management and privacy technologies current projects.
Note: This section should be read in association with the 4th Draft Agenda of the 20th meeting of ISO/IEC JTC 1/SC 27/WG 5 in Jaipur (India) 2015--10--26 to 2015--10--30

After the above identification of apparent privacy gaps at a strategic level, then at least one of the top priority areas would be the standards addressed by the SC 27 Working Group 5 that impact privacy. SC27 WG5 are a primary source of generic international privacy standards.

In order to address a more detailed gap analysis in this core area covering consumer privacy protection (domestic security), privacy control 24x7, identifiability issues and data sharing / transfer transparency and traceability a gap analysis process and resources would be need to be put in place. While the resourcing issue cannot be addressed in this report, a possible methodology has been drafted for COPOLCO's consideration and is available on request. The associated agenda for the SC27 WG5 meeting in October 2015 shows that the group already have many key liaisons in place as well as 17 standards that would need to be examined for more detailed gaps and 4 study periods under way that might also need consumer contributions.

In addition the privacy protection through security needs to be carefully examined across SC27's work, for example a new work item proposal has just been made on Privacy-specific application of ISO/IEC 27001 – Requirements

6. Proposals for next steps

The following are potential steps for COPOLCO listed in the priority order as that seems appropriate to the reviewer.

6.1. Determine how to secure the consumer perspective through consumer representatives in relevant ISO/IEC/ITU work and in national mirror committees and appoint a COPOLCO Key person in relevant JTC 1-work. .

This particularly needs to address

i. the scarcity of voluntary consumer privacy expertise (hence the need to identify and network effectively among representatives)
ii. the role of use case standards for specific products and services

6.2. Develop a new activity template on an International Standard for Privacy by Design (PiB). This would start from the ISO 9000 plan, do, check, act cycle as the EU PbD Mandate 530 has. The plan do check act cycle would lead to a simpler, easier to understand process than other documents currently being developed within ISO.

6.3 Address priority privacy gap filling areas to be agreed with ISO based on:

i. Standards addressing the security of consumer's domestically used digitally connected devices.
ii. Provision of 24x7 privacy preferences control for consumers via their digitally connected devices (this is also related to i.)
iii. Standards addressing acceptable levels of identifiability and sensitivity of data sets about individuals
iv. Data sharing, trading and transfer traceability and transparency standards

6.4. Determine how the wider standards community beyond ISO and JTC 1 could be addressed to identify privacy gaps that lie elsewhere from the consumer perspective as business processes become increasingly digitized.

6.5. Institute two study periods to consider

i. the role and significance of privacy impact assessment automation systems
ii. the role and significance to privacy impact assessment of standards for products and service vulnerabilities and exploits information capture on an industry wide and industry shared basis

6.6 Agree and communicate the consumer digital privacy needs as described in Annex 1. e.g. by presenting an adapted form of this report at the next plenary meetings of JTC 1 and JTC 1 SC 27.

6.7 Undertake a gap analysis of consumer protection in wearable smart devices.

6.8 Promote better information about the standards on privacy protection to make a broader use of what already exists.

Annex 1 **Consumer Digital Privacy Needs**

1 General consumer domestic privacy needs

Security of domestically used digital equipment (hardware and software)

- Network and system security
- Consumer digital devices security
- Keeping consumer protection up to date
- Sourcing trustworthy apps and applications
- Loss of digital devices
- Consumer device security over a product lifecycle
- Consumer security information

Consumer domestic personal processing privacy control

- Consumer privacy preferences and control in real time (24x7)
- Consumer privacy control in cloud computing services via 3rd party apps
- Consumer privacy control for the Internet of Things including smart domestic appliances and cars
- Consumer privacy control for remote control of Things
- Consumer privacy control when 3rd party responsible persons need to be involved (e.g. parents and carers)

Consumer control over their data sharing over social media

- Consumer privacy control over the social distribution of their shared data
- Privacy controls with respect to those receiving socially shared personal information
- Privacy controls when an individual is identifiable in someone else's shared data

Privacy and intrusive content

- Consumer privacy controls for intrusive content
- Consumer privacy controls for intrusive (false) equipment control commands

Consumer privacy control over data collection by third parties

- Consumer privacy preferences and control in real time (24x7)
- Service impacts when privacy data collection preferences are changed by the consumer
- Consumer privacy preference changes and service interactions
- Maximum consumer protection by default

Privacy in public places (physical and virtual spaces)

- Personal data analysis that removes anonymity
- Anonymity when personal information is collected via sensors

Personal accountability for online views

- Accountability for statements and views made online:

- Direct to individuals
- About individuals in public virtual domains

2 Consumer privacy needs when personal data is transferred and traded once it has been collected

Personal data traceability and transparency to support data protection law

- General personal data transfer traceability
- Traceability of transferred data for consumer consent
  - Consent to new processing purposes
  - Consent traceability within original data processing consents given
- Traceability of transferred data for the purposes of personal data access and correction requests
- Consumer query - “where did you get my data from?"

Managing personal data transfer traceability Requests

- Validation of ‘trace my data’ requests

3 Using Consumer Personal Data (data analysis)

Balancing the right to privacy with the public interest

- Governance
- Engaging stakeholders

Anonymity
Re-identification
Profiling: Building up large personal profiles
Data fitness for purpose
Existing customer or client data analytics
Analysis of personal data from open data
Data analytics to identify or target an individual
Data analytics to identify groups of people
Data analytics for systems

4 Consumer Privacy (applicable to some other areas too)

The Right to be Forgotten
Privacy by Default
Privacy by Design

5 Developing Countries Privacy Needs additional to 1, 2, 3 and 4 above

Currently under development within COPOLCO

6 Privacy Impact Analysis for consumer digitally connected devices

Note on key risk areas that consumer digital device Privacy Impact Assessment 's need to address

- Remote control over device power
- Eavesdropping digital radio emissions from devices
- Data transmission to and from the connected device (security)
- User control of data types passed over networks and remote processing of that data
- User personal data sensitivity
- User control over personal privacy preferences
- User behaviours
- User privacy exposure arising from organisational security breaches

7 Privacy information to be provided to consumers (derived from CEN EN 16750)

Public place privacy awareness notification and signage

Consumer product/service information

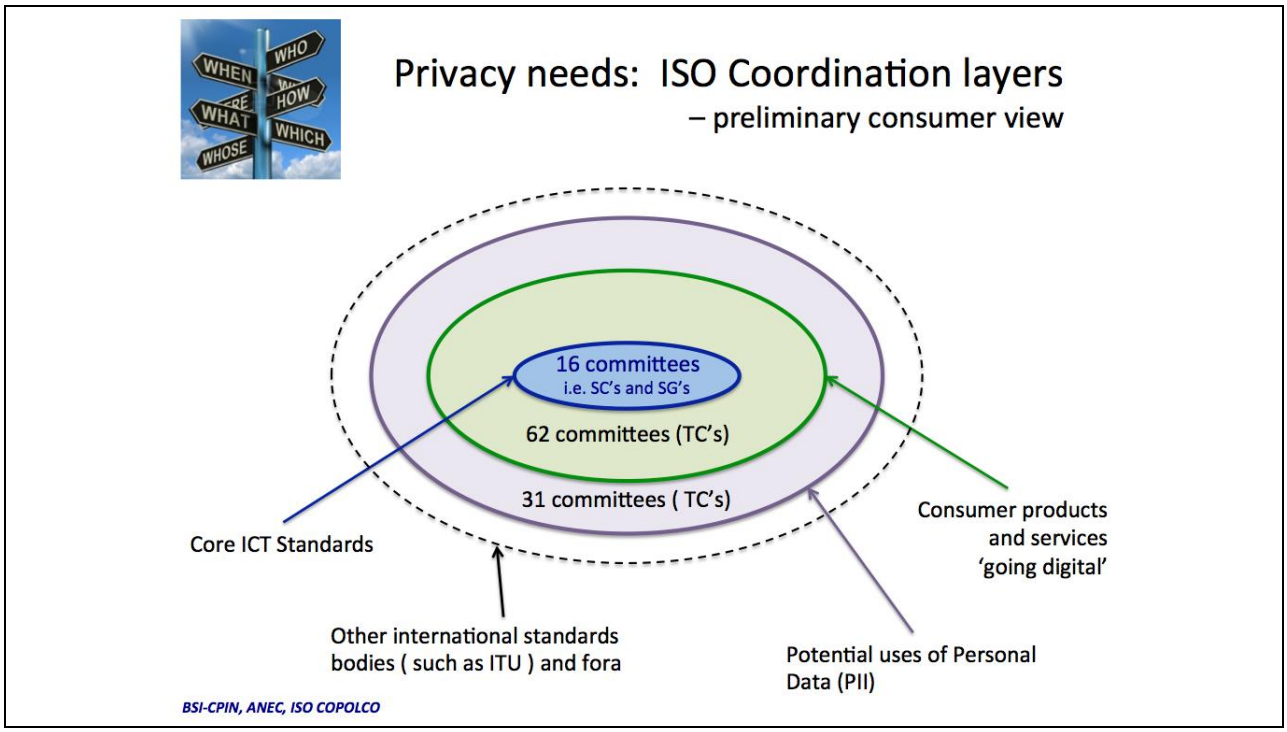
- Consumer Privacy Information Provision Policies
- Summary of privacy impact assessment
- Privacy risks and mitigation actions
- Privacy control instructions
- Privacy labelling
- Privacy and security of domestic equipment maintenance instructions
- Privacy complaints and queries

Annex 2 ISO Coordination associated with meeting privacy needs

A2.1 Preliminary coordination analysis – With a focus on digitally connected devices and goods and services used by consumers a preliminary survey has been undertaken of JCT1 SC's and SG's, the other ISO Technical Committees (TC's) that deal with consumer products[5] and other areas like anti-bribery management that may process personal data (also referred to in ISO standards as Personally Identifiable Information – PII).

Figure 2 provides and an overview of the coordination landscape that ISO is probably facing when it receives the privacy needs gap analysis request from COPOLCO. Detailed lists of committees are provided in Annexes 2.2 and 2.3.

Figure 2 The ISO Privacy Standards Coordination Landscape – a preliminary view

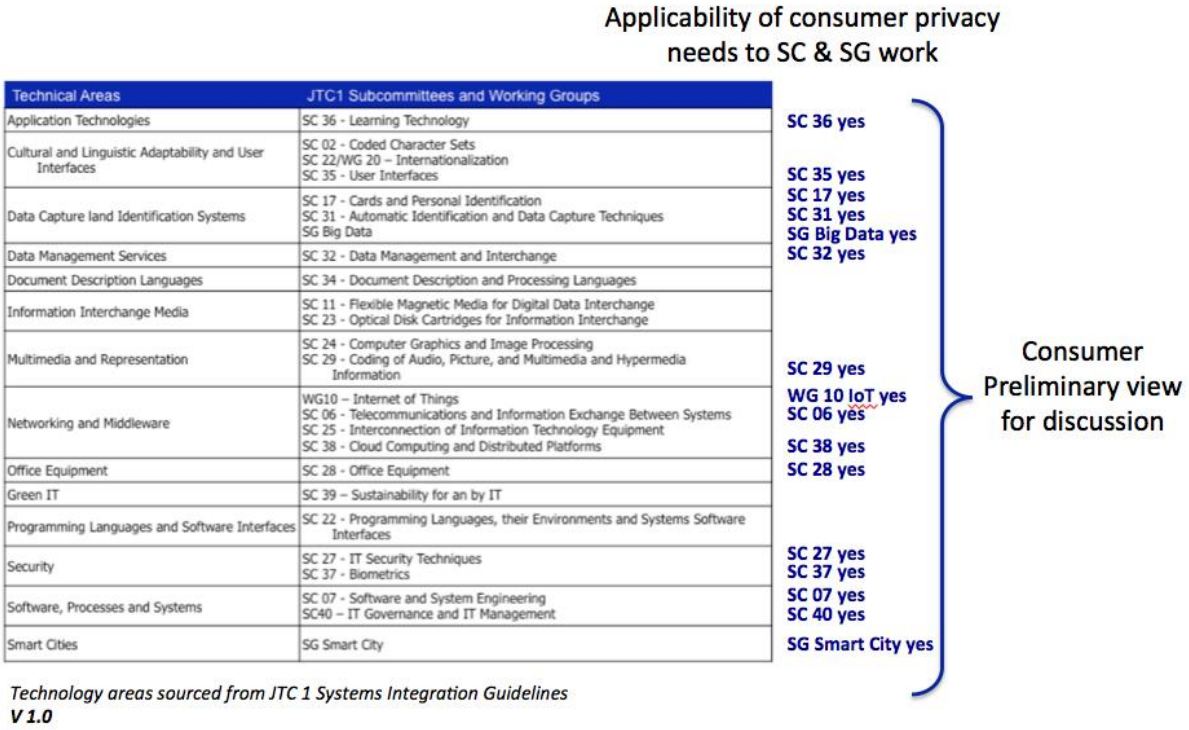


In summary it seems as though up to 16 committees might be involved within JCT1 in order to provide the core standards for privacy to underpin that provided by consumer products. Further there may be over 60 ISO committees involved in setting the right product privacy contexts and over 30 committees involved in setting the right PII processing contexts for privacy by design.

There are other International standards bodies such as the ITU and industry standards fora that also need to be considered and involved.

[5] *Products here is used to embrace both products and services from public, voluntary and private sector providers*

A2.2 JTC1 Committees potentially involved in meeting consumer privacy needs



Technology areas sourced from JTC 1 Systems Integration Guidelines
V 1.0

Editor's note: Please note that a new working-group on Big data is established: JTC 1 WG 9 Big data (it is not an SG any more), and work is being undertaken on social media in JTC 1/SC 37 WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics.

A2.3 ISO Committees responsible for aspects of consumer goods and services and so potentially being involved in context setting for consumer privacy needs

Note: There is a need to prioritize which of these areas has the greatest impact on consumer privacy.

ISO/TC 20 Aircraft and space vehicles
ISO/TC 21 Equipment for fire protection and fire fighting
ISO/TC 22 Road vehicles
ISO/TC 29 Small tools
ISO/TC 31 Tyres, rims and valves
ISO/TC 34 Food products
ISO/TC 38 Textiles
ISO/TC 42 Photography
ISO/TC 68 Financial services
ISO/TC 76 Transfusion, infusion and injection, and blood processing equipment for medical and pharmaceutical use
ISO/TC 83 Sports and other recreational facilities and equipment
ISO/TC 84 Devices for administration of medicinal products and catheters
ISO/TC 86 Refrigeration and air-conditioning
ISO/TC 92 Fire safety
ISO/TC 94 Personal safety -- Protective clothing and equipment
ISO/TC 106 Dentistry

ISO/TC 122 Packaging
ISO/TC 126 Tobacco and tobacco products
ISO/TC 133 Clothing sizing systems - size designation, size measurement methods and digital fittings
ISO/TC 136 Furniture
ISO/TC 137 Footwear sizing designations and marking systems
ISO/TC 145 Graphical symbols
ISO/TC 148 Sewing machines
ISO/TC 149 Cycles
ISO/TC 150 Implants for surgery
ISO/TC 162 Doors and windows
ISO/TC 168 Prosthetics and orthotics
ISO/TC 173 Assistive products for persons with disability
ISO/TC 174 Jewellery
ISO/TC 178 Lifts, escalators and moving walks
ISO/TC 180 Solar energy
ISO/TC 181 Safety of toys
ISO/TC 188 Small craft
ISO/TC 204 Intelligent transport systems
ISO/TC 205 Building environment design
ISO/TC 207 Environmental management
ISO/TC 210 Quality management and corresponding general aspects for medical devices
ISO/TC 211 Geographic information/Geomatics
ISO/TC 215 Health informatics
ISO/TC 216 Footwear
ISO/TC 219 Floor coverings
ISO/TC 222 Personal financial planning
ISO/TC 225 Market, opinion and social research
ISO/TC 228 Tourism and related services
ISO/TC 232 Learning services outside formal education
ISO/TC 241 Road traffic safety management systems
ISO/TC 242 Energy Management
ISO/PC 245 Cross-border trade of second-hand goods
ISO/PC 252 Natural gas fuelling stations for vehicles
ISO/TC 254 Safety of amusement rides and amusement devices
ISO/TC 257 Evaluation of energy savings
ISO/TC 260 Human resource management
ISO/TC 264 Fireworks
ISO/TC 268 Sustainable development in communities
ISO/TC 269 Railway applications
ISO/PC 273 Customer contact centres
ISO/TC 274 Light and lighting
ISO/PC 283 Occupational health and safety management systems
ISO/PC 288 Educational organizations management systems - Requirements with guidance for use
ISO/TC 290 Online reputation
ISO/TC 291 Domestic gas cooking appliances
ISO/TC 292 Security and resilience

A2.4 ISO Committees representing areas that might process PII and so potentially being involved in context setting for consumer privacy needs

ISO/TC 46 Information and documentation
ISO/TC 69 Applications of statistical methods
ISO/TC 70 Internal combustion engines
ISO/TC 121 Anaesthetic and respiratory equipment
ISO/TC 130 Graphic technology
ISO/TC 146 Air quality
ISO/TC 147 Water quality
ISO/TC 154 Processes, data elements and documents in commerce, industry and administration
ISO/TC 159 Ergonomics
ISO/TC 163 Thermal performance and energy use in the built environment
ISO/TC 171 Document management applications
ISO/TC 176 Quality management and quality assurance
ISO/TC 184 Automation systems and integration
ISO/TC 194 Biological and clinical evaluation of medical devices
ISO/TC 199 Safety of machinery
ISO/TC 203 Technical energy systems
ISO/TC 212 Clinical laboratory testing and in vitro diagnostic test systems
ISO/TC 224 Service activities relating to drinking water supply systems and wastewater systems - Quality criteria of the service and performance indicators
ISO/TC 251 Asset management
ISO/TC 262 Risk management
ISO/TC 267 Facilities management
ISO/TC 272 Forensic sciences
ISO/PC 277 Sustainable procurement
ISO/PC 278 Anti-bribery management systems
ISO/TC 279 Innovation management
ISO/PC 280 Management Consultancy
ISO/TC 282 Water re-use
ISO/PC 286 Collaborative business relationship management -- Framework
ISO/TC 289 Brand evaluation
ISO/PC 294 Guidance on unit pricing
ISO/PC 295 Audit data collection
ISO/TC 299 Robotics

Annex 3 Background Material

More detail about these needs is available in 5 ANEC Privacy Guides to be found at:

1. Key Privacy Principles (from the consumer perspective): http://www.anec.eu/attachments/ANEC-ICT-2015-G-007.pdf
2. Key Principles for digitally connected devices privacy impact assessment : http://www.anec.eu/attachments/ANEC-ICT-2015-G-008.pdf
3. Domestic Privacy and the privacy of digitally connected devices : http://www.anec.eu/attachments/ANEC-ICT-2015-G-064.pdf
4. Using Consumer Data – Data transfer, trading and privacy http://www.anec.eu/attachments/ANEC-ICT-2015-G-040.pdf
5. Using Consumer Data (personal data analysis) http://www.anec.eu/attachments/ANEC-ICT-2015-G-009.pdf