AN OUTLINE DESCRIPTION OF THE PROPOSED NEW STANDARD FOR PRIVACY BY DESIGN OF CONSUMER GOODS AND SERVICES

Pete Eisenegger, April 2017

---

1 Overview of the proposed standard

1.1 The need for a requirements standard

The new work item proposal aims to achieve a single standard that allows consumer goods and services providers to address all the lifecycle issues of privacy by design so that through its use and proven compliance consumers can make goods purchases and use services with greater confidence that privacy protection has been designed into the products.

A solution involving several standards to cover a number of phases of product design and update/withdrawal is seen as leading to consumer confusion should only one of several standards be taken up by providers. The digital world is faster in design change, lower cost for design update and so a more integrated process is needed round the continuous improvement cycle of ISO 9001.

Product providers will benefit from an improved trust position in the market compared to the product providers who do not use and comply with the standard.

1.2 A continuous quality improvement process

Software design and update is continuous. So the proposed standard will combine into an ISO 9001 Deeming Cycle (Plan Do Check Act) what was developed as two Safety by Design guidance standards that currently deal with initial product Safety by Design and then Product Recall.

The cycle will consist of a number of requirements pertaining to planning and preparing for product development, then the development and in-company testing phase and preparation for launch followed by product release to the market place and monitoring its performance and issues, and lastly the prioritization and product update development to address issues and improvements.

1.3 Consumer centric

The proposed standard will add to existing ISO Security and Privacy standards the elements needed to account for how we live our domestic lives to give a standard that makes compliance both legal and most importantly practical for consumers.

2 Main purpose of the standard

To provide a standard whereby product (i.e. goods and services) designers and providers can improve consumer trust by demonstrating consumer privacy protection, thereby fulfilling the need to protect consumers from fraud, ransom demands, and other forms of privacy invasion and privacy breaking exploits resulting from lost, stolen and illegally transferred personal data, as well as high-jacking of consumer devices. Particularly of concern is the protection of children and the more vulnerable consumer.

3 Scope of the proposed deliverable

Specification of the design process to provide consumer goods and services that meet consumers' domestic processing privacy needs as well as the personal privacy requirements of Data Protection.

In order to protect consumer privacy the functional scope includes security in order to prevent unauthorized access to data as fundamental to consumer privacy, and consumer privacy control with respect to access to a person's data and their authorized use for specific purposes.
The process is to be based on the ISO 9001 continuous quality improvement process and ISO 10377 product safety by design guidance as well as incorporating in a manner suitable for consumer goods and services privacy design JTC1 security and privacy good practices.

4 Consumer goods and services concept model

There is a need to provide those who use the standard with a concept model and description of the different equipment elements that are addressed in different ways by the design process standard.

The product designers are directly responsible for the design of any consumer hardware and software provided as all or part of the goods and services designed and in addition any application software that has been uniquely created as part of the product where that application software runs on organizational infrastructure, such as corporate servicer farms or Cloud services, where processing occurs outside the consumer's domestic environment.

Then there are 3rd party products that product designers decide to use in order to deliver the overall functionality and performance of their product. Examples being tablet computers on which they mount their 'apps' and routers owned by consumers, and outside the consumer environment cloud services like Amazon's 'Alexa' voice interactive services or business to business services like credit rating and age checking that may be utilized in the product design.

Such 3rd party products are treated differently in the design process as designers can only make use of existing security and privacy capabilities of 3rd party products for their own design.

This section should also provide an overview process flow chart for the 'plan do check act' activities subsequently specified in the standard.

5 Product design governance

Those making use of the standard need to ensure that the right governance arrangements are in place including at a minimum:

- Responsibilities and accountability,
- resources,
- skills and sources thereof;
- budgets,
- project management,
- product objectives,
- key privacy criteria and objectives

This section will also provide practical requirements that allow the smaller more agile product developers to apply the standard effectively when the number of consumers using the product in the market is low.

6 General requirements

The general applicability of law and regulation and standards will be specified and the requirement for product traceability for devices digitally connected to the Internet. This digital traceability requirement is not only applicable for online software updating products but also may be used to enhance product safety by enabling better consumer notification of product risks and recalls.

7 Privacy by Design documentation

There are a great many product documentation requirements bringing together guidance from both Safety by Design standards and Privacy Impact Assessment standards.

8 Definition of the product

The definition of consumer product being either a good or a service will be used.
Requirements will be included to ensure that designers detail their decisions covering:

- A description of the product
- The purposes that the product is designed to fulfil
- The intended users of the product
- An overview of the data flows generated through product use
- Identification of the 3rd party products with which interworking is required to deliver the products overall functionality

9 Definition of supply chain and retail distribution to consumer

Requirements will be established to ensure that product designers consider the security and privacy implications of supply chains and retail distribution channels including

- Supply chain security and privacy implications for any hardware or software components utilized within the product design
- Channel distribution security and privacy implications for product distribution and sale post manufacturing

10 Understanding consumers

This is a vital section of the proposed standard derived from the safety by design standard ISO 10377. It is required to ensure that designers create products that are both legal (as per section 6 above) and just as importantly that products are practical to use with respect to security and privacy protection.

The standard will require designers to undertake descriptions of consumer use scenarios as use cases, and such cases should include intended uses, and other use identified either during the initial design phrase or subsequently as a result of market monitoring of the launched product. The other use cases will include:

- unintended use cases
- misuse cases
- malicious use cases

Further to ensure better consumer understanding the standard will require the consumer types and characteristics relevant to each use case to be documented to enable unintended use to be considered as, for example, should children use a product intended for adults like online shopping.

In addition to focus designers on what is practical for consumers the digital capabilities, and limitations to those capabilities, needed for product security and privacy will be required to be identified by the designers.

Similarly the consumers' human vulnerabilities which product privacy by design should take into account will be required to be identified by the designers.

11 Detailed use cases

Designers will be required to document as a minimum for each use case

- Data flows and processing descriptions utilizing good practices where appropriate from ISO/IEC 19944 Data flows across devices and cloud services.

- Detailed user interactions
- Types of personal data processed and where in the product's modules that would be processed
- The security and privacy preference controls applicable to each use case
- The security and privacy risks to be addressed by the design

12 Consumer requirements setting

From the use cases the designers will be required to list the consumer privacy needs that the design should address. An informative annex providing the COPOLCO list of privacy needs will be provided to assist with this this requirement.

From the list of privacy needs the design process will require detailed design requirements to be set for the product development work. These detailed requirements will include the user security and privacy preference controls to be developed.

13 Establishing the security requirements for the product

Initial design should establish what consumer hardware and software is to be developed and the standard will require the identification of the security requirements for those elements of the product. This section should build on the ISO standard ISO/IEC 19678 BIOS protection as well as any other technology oriented security standards

Further the means of communication with any application software located outside the consumer environment will have been identified in use cases and the security requirements for both the communications and remote application software will be required to be identified. For the application software processed on an organization's own infrastructure ISO/IEC 27034 Application Security is expected to contribute significantly to the proposed standard.

14 Interworking with 3rd party products

The types of 3rd party products with which the product must interwork will be identified as well as specific products and their design levels where that is relevant to the products detailed design.
Then the specific security and privacy control capabilities of those 3rd party products to be used in the product design will be required to be identified by the designer.

15 Product technology vulnerabilities

To enable designers to take account of the inherent vulnerabilities to attack that are present in common technology solutions, the technologies to be used in the design, such as RFID, WiFi, optical cables, mobile phones and their operating systems, cloud services etc. will be required to be identified.

Then the known technological vulnerabilities of those technologies will be required to be identified.

16 Product design tools and support

The standard will address the design practices where these can now be helped by many forms of design tools and good practice guides. So a key part of the design process is to establish:

- sources of design rules,
- design tools
- design good practices

and ensure the standard includes requirements for assessing these support aids are of the right quality and fit for the roles they are expected to play in assisting the design process.

17 Product development testing

The standard will include process requirements for setting test requirements for hardware and software and the final product.

18 Privacy impact assessment

The standard will include privacy impact assessment requirements that build on both current ISO JTC 1 PIA standards work including ISO/IEC 29134, which is more organization centric, and the EU's EN 16571 RFID PIA standard which is more consumer device centric.

19 Product design release

This section will build on the relevant parts of the ISO Safety by Design standard ISO 10377

20 Product incident response plans and incident investigation

Key elements of this section are expected to be built on ISO/IEC 27043 Incident investigation which includes planning for when it is necessary to respond to incidents.

21 Product manufacture / system commissioning privacy reviews

In this section in addition to building on and adapting relevant sections of the Safety by Design standard ISO 10377, there are also sections of the European RFID PIA standard EN 16571 which deal with aspects of practical privacy assessment of system commissioning especially when a system is being enhanced in such a way that new equipment and software has to be added to infrastructure that is at much older design levels.

22 Retail channels privacy reviews

There are privacy implications to how retail channels are involved in getting products to consumers as originally highlighted in the European RFID PIA standard EN 16571 and this section will need to build on that as well as good practice such as that identified by OFCOM in the UK for retail sources of apps.

23 Consumer notifications, labels, signs and consen

Product information for consumers is a key element of privacy by design and ISO/IEC Guide 14 with enhancement for privacy information from, for example, ISO/IEC 29134 PIA standard and the European RFID Signage and Labelling standard EN 16570.

24 Regulatory information

At a minimum this section should contain good practice requirements for the product privacy impact assessment information to be provided to regulators

25 Active market monitoring

Requirements will be established for reporting of privacy / security incidents, investigations, complaints and concerns from professional bodies and the public.
ISO/IEC 29147 Vulnerability Disclosure and ISO/IEC 30111 Vulnerability handling should form the basis for the good practice requirements in this section.

26 Privacy harm action prioritization

This section will provide requirements for establishing clear criteria for action in rectifying product privacy problems and complaints based primarily on the degree of harm that can be experienced by an individual consumer and the number of consumers who would be affected by the issue. The setting of criteria would have to also allow for the impacts on the organization concerned such as brand damage, recompense and security breaches into commercially sensitive corporate data and likely costs of fixing a privacy problem.

27 Remedial action

A key input to the requirements in this section will be ISO 10393 Consumer Product Recall as well as digital good practices for undertaking problem fixing by product design changes, and their validation pre-release, as well as the use of consumer notifications.

Also to be included will be good practice requirements for sales and support channel actions, regulatory notifications, product recall, and product withdrawal.

28 Online software updates

This section will build on the consumer needs for ease of online software update and more detailed requirements identified in the associated ANEC/BSI-CPIN Privacy Guides adopted by COPOLCO.

29 End of life cycle privacy and associated system decommissioning

To address the privacy issues of disposing of consumer hardware and software when the consumer has finished with them requirements will be developed to deal with product disposed as consumer waste, product re-cycling and second hand markets.

Further requirements will be developed to address the issues of data protection when organizations de-commission systems.