ISO FORM 1
ISO TS/P 316

PROPOSAL FOR A NEW FIELD OF TECHNICAL ACTIVITY

PROPOSER:

ISO/PC 317

DATE OF CIRCULATION:

2023-09-29

CLOSING DATE FOR VOTING:

2023-12-22

A proposal for a new field of technical activity shall be submitted to the Office of the CEO (to tmb@iso.org), which will process the proposal in accordance with ISO/IEC Directives, Part 1, Clause 1.5.

Furthermore, a proposal will be considered as complete if every information field is complete and follows the guidelines for proposing and justifying a new field of activity given in the ISO/IEC Directives, Part 1, Annex C.

TITLE

(Please see the ISO/IEC Directives, Part 1, Annex C, Clause C.4.2)

Consumer protection: Privacy by Design for Consumer Products

SCOPE

(Please see the ISO/IEC Directives, Part 1, Annex C, Clause C.4.3)

Standardization of consumer protection in the field of privacy by design for products, including goods, services, and data lifecycles enabled by such products.

PURPOSE AND JUSTIFICATION (Please use the field immediately below or attach an annex.)

(Please see the ISO/IEC Directives, Part 1, Annex C, Clause C.4.13)

Purpose:

The purpose of this proposal is to establish a technical committee that addresses privacy by design of consumer products from a consumer perspective. To achieve this goal, the work on high level requirements for privacy by design in ISO 31700-1, need to be supported by additional standardization projects, addressing the maintenance, the assessment and more detailed implementation of privacy by design.

Specifically:

(1) ISO 31700-1 and ISO TR 31700-2, upon publication, will require ongoing maintenance - documents will need to be updated over time to reflect evolutions in technology, society, and values supporting consumer privacy;
(2) consumer privacy is improved when it is aligned with other values, systems, and frameworks - there is much work to be done to align ISO 31700-1 and ISO TR 31700-2 with other values, systems, frameworks, and standards (see below in the section with the list of relevant standards for examples);
(3) conformity assessment was discussed in PC 317 but not completed - at this time, details regarding ISO 31700-3 as a NWIP will be set forth in a draft Form 4, to be completed by the proposer as ISO 31700-3,
(4) need for privacy standards and interoperability of privacy features has been recognized by PC 317 members, ISO/COPOLCO, and external standards organizations; and

(5) many consumer products, ranging from analogue consumer goods such as food or clothing, to decentralized technology products, include privacy features or associated services that utilize consumer personal information in some manner yet these products are not currently able to demonstrate conformity or be certified to a globally-recognizable privacy standard.

Justification:

Two of the top priorities for ISO for 2030 are to innovate to meet the needs of consumers and to deliver ISO standards when the market needs them. Given the global nature of today's products, there is no question that consumers and organizations (i.e. "the market") need a privacy standard created via international consensus that can apply to products created anywhere, for consumers that may live anywhere. Likewise, the priorities and concerns of consumers around the world are increasingly focused upon how privacy, security, and practical product features embody trust in a product. For example, Pew Research* states that major emerging themes regarding the future of trust in online interactions include, "the nature of trust will become more fluid as technology embeds itself into human and organizational relationships", "trust will not grow, but technology usage will continue to rise" and the current situation is characterized as "less-than-satisfying". In 2020, Pew Research** found that more than half of Americans have decided not to use a product due to *privacy concerns.* And, around 80% of Americans feel that they lack control over their technology products and are concerned about data collection and how that data is used.

Globally, these sentiments are echoed, and generally, ISO/COPOLCO appears to support the creation of a TC that is focused upon consumer privacy protections, especially in relation to technology-enabled products. In its Master Project Overview, version 2020-03-31, ISO/COPOLCO states: "In this digitally pervasive 21st century, protection of consumers' private lives from digital intrusion and harm, as well as any loss of consumer rights, is fundamental to consumer trust in the digital world. If consumer trust is undermined, many of the benefits of digital technology could be delayed or not achieved in full." Furthermore, ISO Strategy 2030 sets forth that, "The growth of digital infrastructures and the integration of digital technologies with other more traditional technologies are rapidly and significantly changing the way people live and work around the world". Given the ever-increasing pace of technology and consumer product development, as well as the already mature and demanding markets for technology-enabled consumer products, it is incumbent upon ISO to commence standards development work as soon as possible to meet these needs and concerns. Meeting these needs and concerns is well-supported for positive and constructive reasons, but justification also arises from the consequences of failing to protect consumer privacy from technology-enabled products.

Members of ISO/PC 317 have commenced significant work to address the consumer issues in this space, and in commencing such work, acknowledge that there is much more to be done. They have analysed early in the development of the committee, that with a Project Committee the task at hand was to address the challenges exposed in the area through developing high-level-requirements, which it subsequently published, alongside with a set of use-cases. However, it was very clear, that the full mandate and request of the TMB could not be fulfilled through a PC. There is an appendix attached which references historical document reflecting on this discussion.

On 6 July 2022, a consultation with WG22 of ISO/COPOLCO further helped establish and describe the purpose of a new TC as a body capable of addressing new and emerging horizontal issues in privacy for consumer products. The report (COPOLCO WG22/N6 CONFIRMED MINUTES OF THE CONSUMER STANDARDS ACTION WORKING GROUP) of this meeting states: "[PC 317] emphasized the consumer focus and privacy neutrality of the discussion and pointed out that privacy and consumer protection issues are rising in importance and scope and that certain technologies (e.g. NFTs) and business models (e.g. DAOs) are advancing without standardization." Subsequently, in this meeting, members were invited "to consider mechanisms to ensure continued consumer protection in privacy issues, especially for emerging technologies" and the members reached a consensus to suggest that PC 317 become a permanent TC as a mechanism to ensure continuing consumer protections. This consensus suggestion was then presented to ISO/PC 317 in July 2022, and ISO/PC 317 subsequently agreed to proceed pursuant to Resolution 60/2022: Preparation of Proposal for New Technical Committee.

Overall, justification for a TC is also significant because the study and operationalization of privacy features is immature compared to some of its technology-focused counterparts, such as cybersecurity; that knowledge

and practical gap must be closed by providing a long-term and dedicated forum for privacy-centric work. Therefore, this TC will serve to directly protect consumer privacy through its own standardization work, and will indirectly protect consumer privacy through more complete and mature technology systems created as a result of liaison and other collaborative efforts between this TC and related bodies that also work on technology-enabled products or systems.

*https://www.pewresearch.org/internet/2017/08/10/the-fate-of-online-trust-in-the-next-decade/

**https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

PROPOSED INITIAL PROGRAMME OF WORK (Please use the field immediately below or attach an annex)
Please see the ISO/IEC Directives, Part 1, Annex C.4.4 and C-4.5)

For each item, the initial work programme shall define the deliverable type and target dates. The initial work programme shall also assign priorities to the different items.

1 IS- Development and publication of a corresponding standard on the conformity assessment of ISO 31700 in coordination with CASCO, starting in 2023 (cf. attached draft expert contribution of a Form 4 for Conformity Assessment of ISO 31700-1)

2 TR -Overview of Areas for Privacy by Design for Consumer Goods and Services, See original Form 4 on the establishment of PC 317 for numerous further areas initially envisioned for standardization, that should be reviewed (Document N2 of PC 317) as well as emerging issues in the field, such as trustworthiness and artificial intelligence, starting in 2023

3 – IS - Development and publication of standards for privacy by design with more specific requirements, such as (among others) use case specific standardization, e.g. see above, or e.g. Privacy by Design for Decentralized Technology Products, starting in 2024

4 – (Systematic) Revision/Evolution of 31700-1 and 31700-2, including ongoing Stewardship and public communication regarding 31700-1, 31700-2, starting (at the latest) in 2028

RELATION OF THE PROPOSAL TO EXISTING INERNATIONAL STANDARDS AND ON-GOING STANDARDIZATION WORK

☒ The proposer has checked whether the proposed scope of the new committee overlaps with the scope of any existing ISO or IEC committee or JTC1 sub-committee

☐ If an overlap or the potential for overlap is identified, the affected committee has been informed and an agreement has been reached between proposer and committee on
   i. modification/restriction of the scope of the proposal to avoid overlapping,
   ii. potential modification/restriction of the scope of the existing committee to avoid overlapping.

☐ If agreement with the existing committee has not been reached, please explain why the proposal should be approved.

A consultation with ISO/IEC JTC 1/SC 27 has been conducted and the results of this consultation are attached.

☐ Have proposals on this subject been submitted into an existing committee and rejected? If so, what were the reasons for rejection?

Click or tap here to enter text.

LISTING OF RELEVANT DOCUMENTS (SUCH AS STANDARDS AND REGULATIONS) AT INTERNATIONAL, REGIONAL AND NATIONAL LEVEL

(Please see the ISO/IEC Directives, Part 1, Annex C, Clause C.4.6)

There are a number of ISO and ISO/IEC documents and standards available that address certain parts and aspects of the work TC 317 is going to undertake. For example, ISO 31000 does address the generic risk management approach, but does not take into account the specific perspective of Privacy by design for consumers, at the product level. As such it will serve as a building block, and a reference point for proposed work of the TC. The task of the TC will then be to use those documents as a valuable starting point to form standards from the consumer perspective, developing a more comprehensive viewpoint.

Relevant documents include, but are not limited to:

- ISO/IEC JTC 1/SC 27/WG 1 standards (ISO/IEC 27000 - family of standards). ISMS plays a vital role for privacy by design, and is already mentioned in the ISO 31700-1, where is serves as a starting point in the requirements.
- ISO/IEC JTC 1/SC 27/WG 5 standards, especially ISO/IEC 29100, ISO/IEC 29134, ISO/IEC 29151. The set of WG 5 standards in the space will be strongly considered in developing standards in a new TC 317.
- ISO 9000 (family of standards) for quality management
- ISO 31000 (family of standards) for risk management
- ISO 17000 (family of standards) for conformity assessment
- ISO/IEC 20000 (family of standards) for IT service management

Privacy and Data Protection regulation and in the different NBs (cf. ISO/IEC JTC 1/SC 27/WG 5 SD 2 List of Privacy Reference Documents, freely available via SC 27 Website) as well as national policy frameworks, must also be considered.

Such as:

E.g. GDPR, CCPA, NIST 800 series

LISTING OF RELEVANT COUNTRIES WHERE THE SUBJECT OF THE PROPOSAL IS IMPORTANT TO THEIR NATIONAL COMMERCIAL INTERESTS

(Please see the ISO/IEC Directives, Part 1, Annex C, Clause C.4.8)

The following countries being P- and O- members of PC 317, and potentially additional NBs:

- Bulgaria
- Canada
- China
- Germany
- Italy
- Japan
- Kazakhstan
- Korea, Republic of
- Netherlands
- Portugal
- Russian Federation
- Saudi Arabia
- South Africa
- Spain
- Switzerland
- United Kingdom
- United States ANSI

- Argentina
- Austria
- Colombia
- Cyprus
- Czech Republic
- Denmark
- Finland
- France
- Hungary
- Iceland
- India
- Indonesia
- Iran, Islamic Republic of
- Ireland
- Jamaica
- Jordan
- Luxembourg
- Mauritius
- Mexico
- New Zealand
- Philippines
- Senegal
- Singapore
- Slovakia
- Thailand
- Trinidad and Tobago

LISTING OF RELEVANT EXTERNAL INTERNATIONAL ORGANIZATIONS OR INTERNAL PARTIES (OTHER THAN ISO AND/OR IEC COMMITTEES) TO BE ENGAGED AS LIASONS IN THIS WORK
(Please see the ISO/IEC Directives, Part 1, Clause C.4.9)

- W3C
- IETF
- DIF
- WEF
- ANEC
- COPOLCO
- CIOSC
- UNECE
- Global Privacy Assembly
- OECD
- ITU

IDENTIFICATION AND DESCRIPTION OF RELEVANT AFFECTED STAKEHOLDER CATEGORIES
(Please see ISO Connect)

	Benefits/Impacts/Examples

Industry and commerce – large industry	A structured approach to designing and operationalizing privacy features for consumer products to ensure products are safe, secure, trusted, and aligned with consumer expectations along with other organizational programs, systems, or policies. Applicable to any industry, market, or supply chain participant.
Industry and commerce – SMEs	A structured approach to designing and operationalizing privacy features for consumer products to ensure products are safe, secure, trusted, and aligned with consumer expectations. Applicable to any size organization, industry, market, or supply chain participant.
Government	With regard to government products made available to its constituents (i.e. consumers), a structured approach to designing and operationalizing privacy features for consumer products to ensure products are safe, secure, trusted, interoperable, and aligned with consumer expectations. Applicable to any industry, market, or supply chain participant.
Consumers	A structured approach to designing and operationalizing privacy features for consumer products to ensure products are safe, secure, trusted, and aligned with consumer expectations. This structured approach will provide consumers with a consistent framework to recognize when privacy needs are or are not met by products. Applicable to any industry, market, or supply chain participant
Labour	An increasingly virtual, distributed, and cross-border workforce would benefit from a consistent set of international best practices around privacy at work, and in the workplace, where many consumer goods are repurposed into business tools. Applicable to any organizational labour personnel.
Academic and research bodies	Academic and research bodies would benefit from aligning international best practices in privacy design and privacy engineering for consumer products. Academic and research bodies would also benefit from the international establishment of privacy (by) design and privacy engineering as distinct fields of study and research applicability. Applicable to all business, technology, commerce, and consumer protection disciplines.

Standards application businesses	Specialized standards groups such as W3C and country-level or local-level standards bodies would benefit from a harmonized privacy approach to technology-enabled product standards, through a dedicated international standards technical committee for privacy design and privacy engineering for consumer products (i.e. privacy by design). Further, auditors, consultants, and other standards-adjacent bodies would benefit from the active alignment of privacy with matters of service management, cybersecurity, and consumer protection.
Non-governmental organizations	NGOs provide services to consumers that may involve technology and privacy, including provision of access to digital and telecommunication services, along with other community services. Further, NGOs may want to create or facilitate community groups needing governance and guidance related to privacy. NGOs that provide services would benefit from best practices guidance related to the selection, application, and deployment of any technology-enabled products, or other non-technical products that nonetheless implicate privacy of individuals receiving the services. NGOs that facilitate the creation of communities would benefit from best practices guidance regarding protection of consumer privacy in novel applications of community, centralized, or decentralized governance. Applicable to a wide variety of NGOs.
Other (please specify)	**Academia (non research)**: Teaching faculty that is not engaged in formal academic research lacks an authoritative and established repository for knowledge related to privacy design, privacy engineering, or the application of privacy values in the context of consumers interacting with products. As products increasingly transcend borders, increasingly become interoperable, and gain increasing economic significance, it is incumbent upon teaching faculty (approximately half of all secondary educators in North America) to educate students in this space and do so from a knowledge base that was created via international consensus. Applicable to all teaching faculty specifically teaching privacy, or more generally teaching product design or business management. **Sustainable Development Goals for society at large:** Via United Nations SDGs, this standards activity is intended to protect consumer privacy and increase trust in technology and serves to support: Goal #8 to promote sustained and inclusive employment and economic growth for all; Goal #9 to build resilient infrastructure and foster innovation; Goal #16 to promote peaceful and inclusive societies.

EXPRESSION OF LEADERSHIP COMMITMENT FROM THE PROPOSER

(Please see the ISO/IEC Directives, Part 1, Annex C, Clause C.4.12)

Click or tap here to enter text.

☒ **The proposer confirms that this proposal has been drafted in compliance with iso/iec directives, part 1, annex c**

BSI commits to providing full secretariat support to the new Technical Committee.

SIGNATURE OF THE PROPOSER

This proposal is submitted by the ISO/PC 317 Chair on behalf of the ISO/PC 317 members, and in collaboration with BSI, as Secretariat of the PC and proposed Secretariat to the new TC.

Jan Schalloboeck, ISO/PC 317 Chairman

COMMENTS OF THE ISO CENTRAL OFFICE (IF ANY)

Click or tap here to enter text.