ISO/IEC JTC 1/SC 17
Cards and personal identification
Secretariat: BSI

Document type: Contributions

Title: SC17 - Comments on Draft ETSI TR re RFID 1

Status: Comments recieved from the Canadian National Body in response to SC17 N 3968.
The comments have been passed to the European Standardisation Organisations, (ESO).

Date of document: 2010-08-24

Expected action: INFO

Email of secretary: chris.starr@ukpayments.org.uk

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1sc17

Commenting template

Date : 2010/08/24	Document: DTR07044v006

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
[CA] 1	3.1 (information security incident)		Ge	An information security incident may involve more than just access to stored or in-transit data. Harms arising from a security incident are typically described as (unauthorized) disclosure, modification, removal, loss or destruction	Amend definition to include the additional harms	
[CA] 2	3.1 (radio interception range)		Ge	Radio interception involves more than just obtaining knowledge of the content of a transmission – it also includes the fact that a transmission has taken place, the time and duration of the transmission and possibly who the communicating parties are	Amend definition to reflect the broader issues associated with radio interception	
[CA] 3	Table 1		Te	While recognizing that this is an EU-centric document, and that the principles listed in Table 1 (with the exception of "equality of regime" and "anonymity" are taken directly from the OECD Guidelines, there are several fundamental privacy/data protection principles which are not given the same prominence as those listed or which do not seem to be mentioned at all, specifically "consent", "retention limitation" and "challenging compliance"	Additional root principles (i.e., "consent", "retention limitation" and "challenging compliance" should be added to this table. Possible text for the principles: "Consent: the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where otherwise specified by law" Subsidiary principles: Consent may be revoked at a later date The greater the sensitivity of the data, the stronger the consent required	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
					"Retention limitation: Personal information shall be retained only as long as necessary to fulfill the stated purposes" "Challenging compliance: Individuals shall be able to initiate privacy compliance-related complaints directly with the host organization or entity" (given that this is an EU-centric document, reference could also be made to the ability of individuals to complain to an independent data protection authority) Text for the "impact on RFID" column already exists in some cases (e.g., for consent) but in some cases, additional text will need to be developed	
[CA] 4	Table 1	Openness	Ed	The means to establish the existence and nature of personal data generally refers to that in the possession of, or under the control of, an organization	Amend to read "…nature of personal data in the possession of the organization" or words to that effect	
[CA] 5	7.2.1	5	Te	The second sentence in this para states "…the person is assumed to control release of personal data". Given the challenges that new technology (including RFID) poses regarding what constitutes personal information, and given the challenges posed by the potential for a rise in machine-to-machine, or device-to-device,	Some sort of caveat should be added to this para to indicate that there will be other scenarios where the assumption re individual control is not valid	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				communication, this may not prove to be a valid assumption over time.		
[CA] 6	7.2.1	6, 7	Ge	These paras state that not only the recovered data needs to be protected but also asserted data and the links between the two data types. This raises a number of issues including: 1) at what point does the data that can be recovered, asserted, etc. cease to be personal information (or does it cease to be PI)?; and 2) the number of organizations that could be involved in the processing of this data and what their responsibilities are for protecting the data	These issues should be the subject of further study by the ESOs	
[CA] 7	7.2.1	7	Ed	The text "…and needs to allow for informed consent" is not the best choice of words – the control of release of data must be based on informed consent (unless otherwise allowed for by law)	Amend last line to read "…and needs to be based on informed consent"	
[CA] 8	Table 3	DPPO-2	Ge	Operators of RFID systems are not only responsible for the personal data collected through the system – they are also responsible for the proper processing of that data (even if the processing is done by a third party on their behalf (data processor versus data controller)). Operators must ensure that any organization processing data on their behalf also conforms with the relevant legislation and regulations (in the EU, this is done via mechanisms such as Binding Corporate Rules)	The "intent" portion of this objective should clearly articulate this extended responsibility	
[CA] 9	Table 3	DPPO-4	Ed	The second para, second list item (under "Intent") appears to be missing text – it ends "…as well as, among others" – "among others" what? There also appears to be text missing from other paras and list items in this objective, as well as in other locations throughout the document (e.g., DPPO-5,	Review and add appropriate text The entire document needs to be carefully reviewed to find	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				DPPO-10 and so on). This makes it difficult to comment on these portions of the text	and correct other instances of missing text	
[CA] 10	Table 3	DPPO-5	Ge	The wording in the fourth para (under "Intent"), dealing with consent for use of data in commercial and public services, is unclear. While the preference is for freely given, specific informed consent, most privacy/data protection legislation and regulation makes allowances for implied consent, both in commercial and public services and in some instances (such as law enforcement) permits processing (e.g., collection, use, disclosure, etc.) of personal data without consent (which appears to be addressed by the text in the fifth para)	The wording in this para should be amended to more clearly indicate that the notion of implied consent applies in more than just safety and public services. Potential wording could be: "Whenever possible, operators of commercial services should obtain consent for the use of personal data. In some circumstances, implied consent may also be acceptable as part of the user's contractual agreement with the service provider. The same is true of safety and public services."	
[CA] 11	Table 3	DPPO-5	Ge	The wording of the fifth para (beginning "Data collection without consent…") is unclear	Suggest amending the text to read something like: "Data collection without consent: National regulation may provide for exceptions to the requirement to obtain consent to the collection of personal information."	
[CA] 12	Table 3	DPPO-6	Ed	Unnecessary text	Under "Intent", remove "Data collection methods"	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
					A similar deletion can be made under DPPO-9	
[CA] 13	Table 3	DPPO-7	Ed	The term "conservation principle" is more commonly referred to as "retention limitation principle"	Amend the third list item to use the more common term	
[CA] 14	Table 3	DPPO-7	Ge	The meaning of the last list item (under "Intent") is unclear. Is this suggesting that an operator should refrain from collecting information which, when combined with other information that might be available to the operator (and not just information in a database), could be used to identify an individual? If so, then say so	Review and amend text for clarity along the lines of the text in the comment field	
[CA] 15	Table 3	DPPO-10	Te	Even a tag that only contains an ID can pose privacy risks. The ID in the tag can be used to "identify" persons of interest (e.g., the tag ID is detected at an anti-government protest) and at some point in the future may permit the linking of the tag ID to a real identity (and there is a risk of a "false positive" if the tagged item is loaned to another individual)	While it may not constitute personal information as commonly understood (i.e., name, address, etc.) – as opposed to personal information as defined in legislation – the processing (collection, use, disclosure, etc.) of the tag ID can pose privacy risks. These should be acknowledged in this DPPO	
[CA] 16	Table 3	DPPO-10	Ge	The meaning of the phrase "data collection finality" in second para, sixth line, is unclear	Clarification is required	
[CA] 17	Table 3	DPPO-10	Ge	There appears to be text missing from the fourth para	Review and add text as necessary/appropriate	
[CA] 18	Table 3	DPPO-10	Te	Is there any particular reason why tag content deletion by overwriting is accomplished using zeros? Why not ones, or some reserved random pattern?	Clarification is required	
[CA] 19	Table 3	DPPO-11	Te	The distinction between the two scenarios outlined in	A note should be added	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				this objective (i.e., "work" and "not work") is not always clear (e.g., employees take RFID-enabled access tokens home; employers permit limited personal use of RFID-equipped corporate assets). In these instances, tag disabling is not an option (unless it can be done for pre-determined periods of time, or the tag can be re-enabled). Other means of "silencing the tags" should be considered/provided for in such circumstances	explaining that use cases/scenarios may overlap and that this needs to be taken into account when designing/implementing/ operating RFID systems	
[CA] 20	Table 4	All	Ge	The numbering of the objectives is incorrect – it jumps from S)-7 to SO-9	Correct objective numbering	
[CA] 21	Table 4	SO-3, SO-4	Te	The distinction between these two objectives is not clear Suggest that data confidentiality is also a security functional requirement for SO-4	Clarification is required Add "data confidentiality" to the list of security functional requirements	
[CA] 22	Table 4	SO-12	Te	Consider this objective to be too limited in scope – no action of the system should expose a user to harm (which includes, but is not necessarily limited to, identity theft/fraud, discrimination, embarrassment and so on)	The objective should be broadened to be more inclusive of other potential harms	
[CA] 23	8.2	All	Te	The link between the threats listed in this sub-clause and those listed in sub-clause 8.1 and 8.4 is unclear The distinction between threats T1 and T2 (note that T4 is a duplicate of T2), and threats T9, T13 and T20, is also unclear T9 is listed twice Suggest that T25 is an instance of T24 and is essentially a duplication of T24	Clarification of how sub-clauses 8.1, 8.2 and 8.4 relate to one another is required The distinction amongst the threats noted needs to be clarified Duplicate entries should be deleted	
[CA] 24	8.2	All	Ge	Given the saying "a picture is worth a thousand	For consideration	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				words", it might prove useful to incorporate a system diagram (along the lines of Figure 5?) and indicate where in the system the threats listed in this sub-clause might materialize		
[CA] 25	8.2	T-17	Te	It is not clear how this is a threat	Clarification is required	
[CA] 26	8.3		Te	A system can have vulnerabilities even if they are not exploited – it simply means that an (hopefully) identified risk has not materialized	Suggest deleting the second sentence	
[CA] 27	Table 5	All	Te	Is the list of threats (8.2) intended to be exhaustively mapped against the vulnerabilities listed in this table (i.e., are T18, T19, T20 and T33 the only threats capable of exploiting V1) (suggest that T24, T25 and T29 are also relevant threats))? Canada can provide additional input, if appropriate, once this is resolved A similar comment applies to Table C.1	Regardless of whether the mapping is intended to be exhaustive or not, an appropriate caveat should be included in the text (perhaps as part of 8.3?). See C.3, fifth para, first sentence for possible text	
[CA] 28	Table 5	V6	Te	The link between the vulnerability and T11 is unclear	Suggest deleting T11 as a threat	
[CA] 29	Table 5	V14	Te	If the text is understood correctly, the term "data correction" is being used in the sense of allowing an individual to request that data about them be corrected (because it is factually incorrect). If so, then the link between the vulnerability and T9 is unclear	Clarification is required	
[CA] 30	8.4.1	2	Ed	Examples, or ranges of examples, are normally expressed as "from…to…" – there appears to be text missing from the first sentence of this para	Review and add text as necessary/appropriate	
[CA] 31	8.4.1	2	Te	It is not clear that tag emulation will necessarily lead to the purchase of a particular product – customers usually rely on other cues (e.g., labeling, etc)	Clarification is required	
[CA] 32	8.4.1	Scenario	Te	The scenario seems to be incomplete – there is no indication of what the attacker might do once he/she	Review and expand the	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				learns about the EPC number and product type	scenario to include at least one example of what an attacker might do after the association has been revealed	
[CA] 33	8.4.2	1	Ed	Choice of terms	Amend last line to read "…reputation, financial loss,…"	
[CA] 34	8.4.4	1	Te	The use of the term "private" is incorrect – the more appropriate term is "personal". Note that personal information can be both public (e.g., listing in a phone book) and private (e.g., sexual preferences). Personal information can also vary in sensitivity from less sensitive (e.g., phone book listing (usually)) to very sensitive (e.g., financial or medical information). There is, however, a distinction in how these 'types' of personal information are viewed in terms of privacy/data protection legislation Note that there are a number of other instances in the text where "private" is used instead of "personal" (e.g., 12.3.1, page 76)	Amend second line to read "…of a personal or sensitive…" Review entire document and replace "private" with "personal"	
[CA] 35	8.4.7.1	Note	Te	The range at which RFID tags can be read has always been a point of contention, regardless of what standard the RFID technology adheres to/is based on (see, for example, http://www.networkworld.com/news/2010/072910-black-hat-rfid-passports.html?source=nww_rss)	It may be more appropriate for this note to be more generic, and to simply acknowledge that actual read ranges are greater than those specified in the standards, or as claimed by vendors	
[CA] 36	8.4.7.3	1	Te	Understanding that the premise behind EPC was to provide for both unique and non-unique codes, there can also be "constellations of unique tag identities", and there can also be mixed constellations	Amend second line to read "…of unique and/or non-unique…"	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
[CA] 37	8.4.7.3	Note	Te	While tracking for the purposes of service delivery is generally thought of as being consensual, there have been any number of studies that indicate that individuals do not read terms and conditions of service level agreements, privacy policies, etc. – so the degree of consent is arguable. Where tracking becomes an issue is when it is used for secondary purposes (e.g., targeted advertising)	Consider adding a second note that points out that tracking for secondary purposes may not be perceived as a desirable trade-off	
[CA] 38	8.4.7.5		Te	As written, this sub-clause appears to be describing a denial-of-service attack (i.e., resource consumption) – a replay attack generally forms part of a spoofing or masquerade attack	Review and amend the text to more clearly describe a replay attack	
[CA] 39	8.4.7.6	1	Te	It may not be appropriate to state that "the payload of an RFID tag is insufficient to carry a virus" – claims were made in 2006 by researchers who claimed to have embedded a virus in the tag payload (see http://www.rfidvirus.org/) – it should be noted, however, that there was a fair bit of debate about the validity of the claims. In addition, RFID tags that form part of a sensor may have larger payloads	Amend second sentence to read something like "It may be possible for the payload of an RFID tag to carry either a virus or the trigger for or link to one."	
[CA] 40	Table 6	All	Ge	This table seems to be out of place here – the discussion of standardization gaps does not occur until Clause 12	Suggest moving this table to the end of Clause 12	
[CA] 41	Table 6	List item O, P	Ed	Should the text under "standardization gap" read "Open system…"?	Review and amend as appropriate	
[CA] 42	9	Title	Ed	The title should read "Privacy and Data Protection Impact Assessment (PIA) Outline" There are other instances in this clause where a similar change is required in the text	Review entire clause and amend text as appropriate	
[CA] 43	9	3	Ge	It is not clear what the phrase "definitive version" refers to	Clarification is required	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
[CA] 44	9.1	6	Ge	A properly conducted security threat and risk assessment should also address risks arising from activities of legitimate insiders	Suggest amending the second sentence to read "The PIA includes privacy risks arising from…"	
[CA] 45	9.1	8, second list item	Ge	The meaning of the phrase "user-centred design" is unclear	Clarification is required	
[CA] 46	9.2	1, first Note	Te	It is not true to state that "disruptive technologies do not have negative connotations" – they can have significant negative connotations with respect to privacy (e.g., surveillance, tracking, etc.)	Amend Note to read "Disruptive technologies can have negative connotations."	
[CA] 47	9.2	1, seventh list item	Ed	All of the other list items in this para are presented as complete sentences – this one is not	For consistency, amend text to form a complete sentence	
[CA] 48	9.4.2	2	Te	It is somewhat premature to present standardization gaps in this sub-clause when the analysis to identify those gaps doesn't appear until Clause 12	Move this text to an appropriate place in Clause 12	
[CA] 49	9.4.4.1	All	Te	The descriptions of the various data protection principles (e.g., purpose specification) appear to mixing text from different principles. For example, the purpose specification principle refers to "limiting the collection of personal information…" – this is really the "collection limitation principle (note that there appears to be text missing which may affect this comment. Similarly, the collection limitation or use limitation principles – as defined in the OECD Guidelines – do not refer to the length of time personal information may be retained (in PIPEDA, this is covered by the retention limitation principle). There is also no text describing the "data quality" principle	Review the text for the various principles and ensure that it properly reflects the text in the OECD Guidelines Add appropriate text to the "data quality" principle	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
[CA] 50	9.4.4.1	All	Te	While recognizing that this is an EU-centric document, and that the principles listed here are drawn from the OECD Guidelines, there are several fundamental privacy/data protection principles which are not given the same prominence as those listed or which do not seem to be mentioned at all, specifically "consent", "retention limitation" and "challenging compliance" (see CA3)	See CA3	
[CA] 51	9.4.4.1	2, list item 6 (Rights of data subject)	Ge	Believe that the text "availability of contact information" refers to contact information of an accountable individual within the organization. If so, this text should appear in the previous sub-para	Review and move text if appropriate. Otherwise, reword to more clearly show the link to this principle	
[CA] 52	9.4.4.1	2, list item 7 (Security safeguards)	Ed	Believe the text beginning "prevent unauthorized…" represents examples of security safeguards. If so, this text should be enclosed in parentheses	Review and add parentheses as appropriate	
[CA] 53	9.4.4.1	2, list item 8 (Third party transfer/ processing), 9 (Third country transfer)	Te	In some instances, third party transfer and third country transfer may be the same thing. Regardless, these appear to be specific instances of the use limitation principle (specifically "Personal data should not be disclosed, made available or otherwise used…"	Consider moving this text to form part of 2 (Collection and use limitation/minimization)	
[CA] 54	9.4.4.2	2, list item 1	Te	Temporal privacy is used in this item to refer to "the location of an individual at a discrete point of time". There is another aspect of "temporal privacy" that is not addressed here – the sensitivity of information may vary over time (i.e., something that is sensitive today may not be sensitive ten years from now) A similar comment applies to Table 8, third row (spatial (location) and temporal dimension of privacy)	Consider including a note to this list item to at least introduce this other aspect of temporal privacy Make a similar change to the corresponding entry in Table 8	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
[CA] 55	9.4.4.2	2, list item 4b	Ed	Choice of words	Suggest amending text to read "aggregated (personal) data…" This change should also be made in Table 8, second last row	
[CA] 56	9.4.4.3	1, fourth list item	Te	Suggest that there are other groups of individuals that also require additional consideration with respect to RFID (e.g., seniors, the physically and mentally challenged, prisoners, etc.)	Suggest amending this item to read "protection of vulnerable populations (e.g., minors, seniors and so on)"	
[CA] 57	Table 7	All	Te	Presumably the listing of controls/measures in this table is non-exhaustive. If so, this should be states	Add a caveat to the effect that the controls/measures listed in the table are representative of controls that can be implemented to mitigate the listed risks	
[CA] 58	Table 7	All, third column	Ge	This column refers the reader to Clause 5 for more detail concerning threats and risks associated with the various categories/issues outlined in the table. This reference is incorrect – threats and risks are discussed in clause 8	Amend reference throughout the table	
[CA] 59	Table 7	First row, second column	Ge	There are several options for disposal of information (e.g., destruction, transfer to a new system, archiving) – use of only "destroy" does not acknowledge these other options. Note that any disposal of data needs to be done securely	Amend to read "or otherwise change, dispose of data"	
[CA] 60	Table 7	Second row, second column	Te	Should the text in the last 'sentence' read "Re-use for compatible purposes" – this phrasing would be more in line with text in Table 1 (as written, it may suggest that re-use for incompatible purposes is acceptable)	Consider re-phrasing the text along the lines in the comment text	
[CA] 61	Table 7	Fourth row,	Te	It is not clear how "the length of time for which data is	An additional row should be	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
		second column		kept" is related to data quality – this is a retention limitation issue and should be addressed separately (see also CA3) Note that data retention is also dealt with in the previous row ("collection and use limitation, minimization) – as above, this should be addressed separately	added to this table for "retention limitation". See attached document for possible text for such an entry	
[CA] 62	Table 7	Fifth row, third column	Ge	Inconsistent level of detail There are two other instances of this comment within the table – these should be corrected as well	Additional detail outlining the key threats and risks should be added to this column – possible text can be found at Table 5, V3	
[CA] 63	Table 7	Eighth row, fourth column	Te	The ecosystem components involved in third party transfer/processing are not just limited to backend systems – components such as the architecture are involved in the transfer of information The same comment applies to third country transfer/processing	Review and add other relevant ecosystem components The corresponding column in Table 8 should also be reviewed with this comment in mind	
[CA] 64	Table 7	Ninth row, second column	Te	The text beginning "for the performance…" also applies to third party transfer/processing	Add this text to the "explanation/comments" for third party transfer/processing	
[CA] 65	9.4.4.3	Page 52, last para	Ge	Believe that the reference to Table 4 is incorrect – believe this should be Table 8	Review and amend reference as appropriate	
[CA] 66	Table 8	Fifth row, third column	Te	Tracking is another relevant threat associated with behavioural privacy	Add "tracking" in this column	
[CA] 67	9.4.4.3	Page 54, last para	Ge	Believe the reference to Table 8 in the first line is incorrect – believe it should read Table 9	Review and amend references as appropriate	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				Believe the reference to Tables 3 and 4 in last line is incorrect – believe it should read Tables 7 and 8		
[CA] 68	10.3	1	Ed	Missing word, extra word	Amend third line to read "…and ability to transcend…" Amend sixth line to read "…8 years as RFID…"	
[CA] 69	10.4.1	E.1, E.2	Ge	The text in these two requirement specifications appears to be very similar, especially under "Primary"	Consider making the distinction between these two specifications clearer	
[CA] 70	10.4.1	E.6	Ed	Extraneous text	Remove "specifications and guidelines" from list item text in third column	
[CA] 71	10.4.1	E.9	Te	It is not clear why the fourth column includes the text "Not audible signal" – it contradicts the guidance provided in the next column (list item 2) and in 10.4.2, S.3 It is also not clear why the fifth column includes reference to risks to health – the incorporation of touch or audio communication media is more an accessibility issue, not one of health	Amend fourth column to include reference to audible signals Delete "and RFID systems themselves pose no known risk to health"	
[CA] 72	10.4.2	EL.1	Te	This requirement includes an exception to the location and placement of RFID tag notices (presumably – this is not immediately clear from the text). It is not clear how an RFID field can be "present or measurably present" if there is no RFID system or application installed or operated in the area It is also not clear why the owner/operator of an RFID	The guidance in this specification should be reviewed, and consideration given to adding guidance to address the issues raised in the comment column	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				system that extends beyond the organizational premises would not have an obligation to post – within those premises – some sort of notice to this effect (i.e., that the RFID system or application may extend beyond the premises), especially if "the RFID interrogator system can activate tags outside the perimeter"		
[CA] 73	EL.3	Last column	Te	The guidance provided in this column, list item 4, should be strengthened	Amend to read "Reference to…containers shall be included to ensure that RFID tags in wholesale or bulk purchases, re-used boxes, etc. are visible to the public"	
[CA] 74	10.5	Title	Ge	It is unclear why the term "classified" is used in the title	Clarification is required	
[CA] 75	10.5.2	SL1	Te	The text under "Primary" is more appropriate to location (where), rather than time (when) See also CA71 as it relates to the text in the fifth column	Review and amend text to be more closely related to "when" See CA71	
[CA] 76	10.5.3	SO.2	Te	The onus for ensuring compliance with relevant standards should not be imposed solely on the owner of the RFID sign – sign manufacturers/vendors should also bear some responsibility	Amend guidance to be more inclusive (perhaps under "Secondary"?)	
[CA] 77	11.3	1	Te	Privacy and data protection legislation/regulation typically provides exceptions to the privacy/data protection principles in cases involving law enforcement, national security and so on – this is acknowledged in Table 1 (Collection limitation; Use limitation), for example Similar acknowledgement of these exceptions should	Add text similar to that which appears in Table 1, last column	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
				be included here		
[CA] 78	12.2.2	2 (2.4)	Te	The inclusion of a capability to change read distances creates significant potential security and privacy risks, regardless of who (government, private sector, attackers) effects the change. The implications of such a capability need to be thoroughly examined before being implemented	Use the comment text as a note to be appended to item 2.4	
[CA] 79	12.3.1	1	Ed	It is not clear what "this" (first line, ninth word) is referring to Choice of words	Clarification is required Suggest amending third line to read "…large quantities of…"	
[CA] 80	12.3.1	4(?)	Te	Is it appropriate to reference a particular technical solution (e.g., 32-bit passwords), given the possibility that the solution will change over time (also note reference to 48-bit passwords in Table B.2)?	Amend text to read "The password…"	
[CA] 81	Annex A	Sensor processing (page 79)	Te	Depending on the nature of the sensor data (e.g., location, medical, etc.), "reading the sensor data" may be a genuine concern	Amend text to read "Depending on the nature of the sensor data (which may constitute (sensitive) personal information), reading the sensor data may not be as much of a concern."	
[CA] 82	B.2.1	1; Table B.2, Note 1	Te	The A in the CIA acronym usually stands for Availability, not Authentication, Authorization and Identification	The acronym CIA should not be used in a manner that is not commonly understood. Suggest deleting the acronym and using the full text instead	
[CA] 83	Table B.2	ISO/IEC 18000-3 Mode 3	Ed	Believe the text in the third column should read "For MB01 to 10, locking…"	Review and amend text as appropriate A similar change needs to be	

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Source[1]	Clause (e. g. 3.1)	Paragraph/ Figure/ Table (e. g. Table 1)	Type of comment[2] (e. g. ed)	Comments: Justification for change	Text of proposed change	Final resolution of comment (Will be filled by resolution team)
					made for text in ISO/IEC 18000-6 Type C	
[CA] 84						
[CA] 85						
[CA] 86						
[CA] 87						
[CA] 88						

[1] **Source = Organisation of individual providing the comment.**
[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial **Columns 1, 2, 4, 5 are compulsory**

Canadian contribution to support Comment CA59

Category/Issues	Explanation/comments	Threats and Risks	Ecosystem component involved	Control/measure	Standardization gaps
Retention limitation	The length of time for which the data is kept Note that retention periods may be specified by other laws, regulations and so on (e.g., for financial or medical records)	Retention period exceeds the period of time necessary	Backend systems	Automatic deletion or disabling of data at end of retention period	Details are in clause 12

Canadian contribution to support Comment CA88

Annex D	Table 3	
DPPO-4	DPPO-3	
DPPO-5	DPPO-4	
DPPO-6	DPPO-5	
DPPO-7	DPPO-6	
DPPO-8	DPPO-7	
DPPO-9	DPPO-7	
DPPO-10	DPPO-8	
DPPO-11	DPPO-8	
DPPO-12	DPPO-9	
DPPO-13	DPPO-7, DPPO-9	
DPPO-14	DPPO-10	
DPPO-15	DPPO-10	
DPPO-16	DPPO-10	
DPPO-17	DPPO-10	(Note that second column should read "tag content deletion")

DPPO-18	DPPO-11
DPPO-19	DPPO-11
DPPO-20	No counterpart
DPPO-21	No counterpart
DPPO-22	No counterpart
DPPO-23	No counterpart
DPPO-24	DPPO-2 (?)
DPPO-25	DPPO-3 (?)
DPPO-26	DPPO-3 (?)