DRAFT 2018-11-15 Meeting notes (CR)

Date

2018-11-15

Status of Minutes

DRAFT

Approved at: <<Insert link to minutes showing approval>>

Attendees

Voting

- Andrew Hughes
- Oscar Santoalla
- Jim Pasquale
- Mary Hodder

- Mark Lizar

Non-Voting

- Tom Jones
- Sneha Ved
- Peter Davis
- Sal D'Agostino

Regrets

Quorum Status

Meeting was <<<>>> quorate

Voting participants

Participant Roster (2016) - Quorum is 5 of 9 as of 2018-07-12

Iain Henderson, Mary Hodder, Harri Honko, Mark Lizar, Jim Pasquale (C), John Wunderlich (VC), Andrew Hughes (VC), Oscar Santolalla, Richard Gomer

Discussion Items

Time	Item	Who	Notes
4 mins	- Roll call - Agenda bashing	Andrew Hughes	- presentation from Peter Davis - Airside Mobile on their planned implementation of Consent Receipts - discuss the road map - are there high priority items? - discuss ideas for EIC May 2019 demo and other talks
5 min	Organization updates	All	Please review these blogs offline for current status on Kantara and all the DG/WG: - Director's Corner: 2018: October - Work + Discussion Group Activity There is a wiki page that will hold all the known implementations of Consent Receipts - Please update the page or inform Andrew of your implementation. - TIIME, Vienna, February - EIC, Munich, May - Identiverse, Washington, June

15 min	Demo from Airside Mobile	Peter Davis	

- Airside Mobile - Mobile Passport product - seen in US Airports now - about 5 million users today - Peter joined this year
  - Has advised them from the start to incorporate UMA and Consent Receipts
- Essentially they are dealing with pairwise sharing of information - passports and drivers licenses to start
- High level flow:
  - 'relyingPartyInfo' is the beginning of a 'consent receipt' object

  - The image is for pre-flight information - filing flight plans - from the iOS app
  - 'duration' - a gap in the spec
    - CR has the execution timestamp - no 'validity' or 'end date'
    - Airside includes end dates after which the relying party is required to delete the data
  - Terms of use and privacy policies are exposed to the user
    - In the CR spec, there's no way to specify multiple policies/terms that apply
  - Subject, in effect, issues a license to the RP to use the data
  - Future: will build out a dashboard for the individual to look into their licenses/receipts
- They use CRs in solicitation of data and also an artifact of the sharing
- Q: The privacy policy field is a URL, so the content might change
  - A: They advocate for two forms of URL - one is a URI that includes a timestamp fragment - and one that is a 'current' version URL
- A challenge with DOIs is that they must be registered - motivation in the customer base is probably low
- Q: Any recommendation to use DOI or URN?
  - A: Probably DOI - because the registry/registrar infrastructure is already

30 min	Roadmap ideas for Kantara CIS WG products	All	

Continuation of the product roadmap discussion...

Prep material for 2018-11-15 call:

A new flow chart showing a generic 'agreement-oriented' viewpoint:

https://share.mindmanager.com/#publish/NEsOqIqyWZ2buLfRgPdytSBf9KO1pQpZZMM4J0PS

Andrew's email to prepare for this call:

https://kantarainitiative.org/pipermail/wg-infosharing/2018-November/003156.html

These are some of the questions that came to my mind, to ask at the flow chart steps:
* At each point in timeline what data is offered or consumed?
* What information and metadata should persist? (to record keeping)
* Under different legal bases what information should be provided to the individual?
* What happens at first use? Does something different happen at subsequent use?
* What information is needed to exercising a data subject right? (and is that information recorded anywhere?)

From 2018-11-15 call:

- Sneha notes that their flow is more party-party-consent manager - so the high level 'agreement' flow chart needs adjustment
  - Andrew: Yes. The generic flow chart is intended as a starting point - more specific ones will be developed for different use cases
- Andrew walked through the flow chart
- Q: is the idea of a third party record keeper archivist in play?
  - A: yes - not at this level of detail - because this flow chart does not show who is performing the action, just who is responsible for the action
- Discussion ensued
  - Analysis of any particular use case using the flow chart as a tool
    - The details of what records should be kept are specific to the use case being analysed
  - We will build out a taxonomy of use cases that we analyse
- General sense of the room is that this is a good base model from which we can derive specialized flow charts to suit any use case

From 2018-11-08 call:

Some food for discussion:

- If we believe that the CR should be adjusted to enable general use for any legal basis for processing, what steps are needed (where are the requirements? what are mandatory/optional features? etc)
  - Transformation of the specification into a "Notice Receipt"
- If we believe that 'consent' will become a peer with the other legal bases for processing, then maybe we should leapfrog and look at requirements from ePrivacy Regulation, and take an affirmative position in the marketplace that Kantara Consent Receipts are designed to be fit-for-purpose to address ePrivacy, GDPR and GDPR-similar regulations.
  - Document use cases from specific companies - to give us focus
- Realign thinking towards "Consent Sharing & Information Sharing"
- Is there support in this WG to use the "Contract Law" concepts as the scaffolding/framework for future development of the "Kantara receipt" construct?
  The use cases described last week (in addition to the ones in the github repo) were:
  - Privacy Dashboard
  - Evidence of Action
  - Agreement Details and Transaction Records
  - Standardized Message Data Structure
- Comments
  - Having the concept of "contract" would be helpful
  - GDPR pushes to get away from "data as currency" - the purpose for the interaction is paramount and should be the justification for the 'consideration'
  - **Be very cautious that applying the Contract Law metaphor could overly influence our thinking about how we design and apply consent**
- Address the taxonomy of privacy, notice, control

From 2018-11-01 call:

Andrew led the group through a discussion looking at the central 'agreement' between data subject and data controller in light of basic concepts of Contract Law in the Common Law to see what patterns and insights are available

Andrew has uploaded some material to help the discussion: Product Roadmap Ideas

Blog: Kantara Initiative Work Groups on Data Sharing and Consent

Mind map to go with the blog

Kantara consent high level use cases.pdf

From 2018-10-04 call:

- If the legitimate basis is not 'explicit consent' - but rather legitimate interest, is the concept of 'data receipt' still viable?
- Mark - yes, the current CR was designed to be not confined to 'explicit consent' - so yes, the receipt concept will work for other bases for processing
  - in particular - for updates to privacy notices
- Mark Q: would it be interesting to have addition values for the 'consent type' field? A: YES!
  - Jim: maybe this should go to the Consent Management WG?
- A lawyer at the Seattle event pointed out that it would be useful to capture the actual privacy notice that was agreed by the user.
  - OpenConsent has an alpha product that might suit the purpose
  - There is a systemic problem that needs to be addressed - and capturing the privacy notice won't actually help
  - If there is a strong need for a high value receipt, then it would be very useful to capture the actual notice text
  - So maybe the receipt could have optionality to allow for capture of the notice text.
- WG needs to take some time to discuss the UX - schedule it
  - Tom has posted some examples that could be discussed
  - Mark - OpenBanking has posted UX guidance
- Schedule specific multiple calls for this to discuss what the user should see, and how this translates into the 'receipt' concept
  - Should this WG do a spec or guidance on UX or UI?
  - Should this WG talk about what the 'receipt' means and / or represents?
  - (YES to both question)
- Andrew: suggests first design call on Thursday October 18, 2019 and then every 4 weeks to be kind to the down-under-ers.

Iain: the highest value work item is the lexicon work

10 min	Adding feature requests to next version of spec family	All	- Andrew has set up a github repo for next-version specification backlog items, including use cases: https://github.com/KantaraInitiative/consent-receipt-v-next - Some possible items for next versions: - Structural changes to the spec including a hierarchy of objects that should improve high transaction volume - Integration/association of the new Blinding Identity Taxonomy into the CR Spec family (to inform implementers of potential data categories of interest) - See also this Data Categories infographic: https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf - Recommendations for Customer Journey / UX / UI features - Library of industry-specific or case-specific Purpose categories and example Purpose statements - Expansion of Consent Types to allow for more than just Explicit Consent situations (idea) Optional receipt metadata to assist privacy dashboards in organizing and processing 'bring forward' items (e.g. "remind me to check this share in 3 months") - digi.me product and management have identified six areas for development - consent over period of time (rather than instantaneous consent) - termination/modification of consent from either side - high transaction volume & low per-instance cost - how the 'receipt' fits into accounting systems infrastructures - receipt as the basis for legal matters and actions - UX/UI concerns - for Clinical Trials uses, data holder is required to keep data for 10 years - need to consider longevity of the receipts to go alongside data holdings
5 min	Product roadmap for the demo	All	Target is EIC May 2019
	AOB		
	Next meeting		***** Next call 2018-11-22 10:30 am Eastern Standard Time / 15:30 GMT**