Position Paper:

Title: Do Track - A Do Not Track Use Case

Short Description: This position presents the Standardized of digital transparency to open consent with privacy rights that enable data controls to scale online. The use case presents requirements for specifying human to tech governance interoperability. Focusing on the effort to standardize *digital transparency infrastructure* to enable people to openly use social (decentralized) consent to scale legally and digitally online.

Author: Submitted by Mark Lizar, CEO of 0PN:Consent Public Benefit Consortium, mark@0pn.org

a. W3C: Consent WG – Participant (TBC): Soheil Human (soheil.human@wu.ac.at) Advanced Data Protection Controls

The 'Do Track'- Do Not Track Use Case

Do Track use case provides requirements for semantic interoperability online, utilizing the do track opt-in and out signal.

- In summary, do not track, refers semantically to opting out of surveillance, which is not consent(ric). This position paper argues that the individual would need to opt-in to surveillance, for consent to be possible and to scale data control online.
- Newly published specifications and long matured standards provide the opportunity to implement a decentralized and permissionless data flow, that begins with authorization, for standardized transparency over authority, for consent before authentication.
- This use case utilizes multiple standards and specifications to enable digital transparency, including semantic interoperability.

The key is to the Do Track use case, is a Consent Receipt, which is arguably the ancestor of the first script a human has ever written, represented as a receipt.[i] To this point, it is hypothesized that, "Writing itself may have been invented as a way to create receipts."[ii] Receipts enabled trust to travel with goods for trade between people. In fact, a bank receipt was the innovation that enabled gold to be exchanged without having to transfer it around in late medieval Italy.

- The effort to spearhead privacy standards for international data flows began internationally with the OECD Guidelines for the Trans Border flows of information(ref), which was published in 1980. This led to 2011 ISO.IEC 29100: Security and privacy techniques.[iii] Which is an open/free ISO/IEC specification.
- In 2012, a call to action, to open notice to address the lack of consent online was presented at the Do Not Track & Beyond conference at Berkely. [iv]
- This led to the effort to create a Consent Receipt[v] with a focus on consent in order to contribute to ISO/IEC 29184 Online privacy notice and consent standard, through the Kantara Initiative liaison.
- This is how the 'consent notice receipt' first makes its international appearance, in Annex D.[vi]

Semantic Interoperability Challenge

- At the time it was clear that the challenge was semantics, revealing a big hole in privacy policies, As there were no semantic legal specifications, that scaled online. Key challenges.
    A. Services don't notify of changes to valid state of processing or provide notice of processing. The lack of protocol for asserting providence of individual authority, while impossible to assess the valid state of processing, authority and providence in context prior to authentication,
    B. Any purpose can be provided without a way to verify the purpose or implement certified codes of practices to facilitate more performatice form of digital trust

Scaling Identity Governance Semantics

- It wasn't until the co-launch[vii] of the W3C DPV (Data Privacy Vocabulary Control CG),[viii] a legal semantic ontology for machine readable and executable privacy vocabulary.
- To address the first challenge, Jason Cronks (open) 'Personal Data Categories' were iterated on at Kantara before the DPV took on this task.[ix]
- The DPV subsequently incorporated the consent receipt vocabulary which extended the ISO/IEC 29100 standard with consent notice receipt terminology.

In 2019, ISO/IEC WG 5: SC27 adopted the consent receipt specification, to start working draft 1 of ISO/IEC 27560, Consent record information structure.

This has led to a new effort at the Kantara initiative ANCR (Advanced Notice and Consent Receipt) WG[x] launched in 2020 to operationalize the work. With an overarching notice and consent record and receipt information structure to incorporate multiple community efforts in developing open and accessible records of processing activities.

and, with the ratification of CoE 108 +,[xi] and international and enforceable privacy legal framework, a transparency code of conduct which scales online consent can be implemented. (thus operationalizing privacy for people for consent independently of a services contract for terms and conditions,

The Do-Track use case presents the opportunity of the open public solution components used to engineer and implement the standardized semantic framework. Engineered, through the EU funded Privacy as Expected: Consent Gateway Project.

1. The Notice and Consent Record and Receipt. Mirrored record authorization protocol, implemented prior to authentication, wrapping terms and conditions in an operational privacy policy represented by a consent receipt.
2. Two factor Notice, for proof of knowledge. Which is a notice for a specific purpose, not only a notice for technical permissions on database file in software driven system. This notice has a standard; Consent Button, Rights Button, Reject Button, and can include additional education and awareness requirements, before these buttons can be activated.
3. Once engaged a proof of privacy notice record and consent receipt is generated, with DPV, to provide a receipt for legal evidence of consent, although not technically evidence of consent online without being signed by the Individual, service provider and a verifier, which can be notarized.

The Consent Receipt artefact, can then be used by the Data subject to assert authority and access privacy rights services autonomously in order to affect the flow, access, and control of personal information.

Decentralization is enabled through the monitoring of the controller credential and the performance of privacy rights services.

The Great Security Challenges

Online, it is almost impossible to see what organization, company or beneficiary is behind an online service. This means that people are put under surveillance before they provide consent to surveillance. This presents a security gap where peronal data can be breached, by copying the data and disclosing it to third parties for the purpose of

profiling, tracking, and profiting of personal data. Without standards, people are unable to see these practices and contexts, unable to protect themselves, and unable to trust in the use of personal data technologies like digital identity management.

Misinformation and the co-opting of consent with un-consented surveillance.

For example, Do Not Track, to opt out of surveillance could be reframed as Do-Track, to opt into surveillance.

To make this operational, the prefix of the consent receipt, which contains, the identity, and contact information of the data controller or representative is the core identity record, which is required to be open and transparent in terms of privacy and security risk s.

4. Controller Credential,
    i. The prefix of the consent receipt field format specification, with a few additional fields required to digitally twin the Data Controller credential. Making it extremely easy to technically embed constraints to encapsulate data spaces with a controller credentials. The Notice Controller Credential is in progress at the Trust over IP: Notice and Consent Taks Force. [xii]
    ii. Consent by design The Controller Credential is generated from verified public data to be independently available, or embedded in by a digital service to be automatically discoverable. In this way, a credential can be used to generate records and receipts automatically using authorization defaults. Consent by design, in contrast to the surveillance design pattern of the current Do Not Track features.

The Great Usability Challenge

How can people access or use privacy rights if they can't see or understand them? Without defaults for consent and transparency?

Privacy Icons, industry, sector, or legal location specific, do not scale, each context has its own policy, its location its own culture and law. How can this be addressed?

How can, with a click of a button, permission services to work for my device? How can I click the same Do Track button to restrict data processing to multiple

services, in a single context at once? (i.e. for privacy in a café) How can the Do Track button and 2fN, be implemented with the age appropriate design code of practice?

5. Micro-Credentials
    i. Generated when a consent receipt is signed by one of the privacy stakeholders, and notarized by another.
    ii. It can only be used for the purpose specified
6. Differential Transparency
    - To effectively decentralize notice and consent, each digital interaction and session is authorized prior to authentication.
    - A consent receipt (micro-credential) is generated from the controller credential and compared against the previous receipt, to detect if there are any changes to the valid state of processing.
    - The controller is monitored on several data points, with public authoritative information sources, to provide decentralized privacy assurance with higher performance dynamic data controls.
    - How the differential transparency signal operates.
        - If there is a change in the valid state of privacy and consent a notification is generated by the controller and only when there is a change in the expected state of privacy is a signal generated. and only when there is a material change in the valid state of consent if the flow of personal data disrupted, Through the application of privacy rights, dependent on the legal justification for processing capture in the notice record or consent receipt.
        - The individual is notified of the disclosure, the risks, can mitigate them, and dynamically renew consent, specifying the access to personally controlled and secure information.

In Summary

Do Track signaling represents an architecture in which records and standards are generated that Individuals control and can the used for evidence of consented surveillance and the processing of meta data.

As such, records and receipts provide a method to maintain and exchange a shared expectation of privacy and data control, to monitor the valid state of consent, and to personalize with operational privacy.

The next frontier in this field of work aims to facilitate the public benefits of personal data processing leveraging computational privacy capabilities. For example, micro credentials that provide personal records of processing for machine learning and a privacy AI.

As a result, it is mission and recommendation to support Do Track, and the effort to deploy and develop Two factor Notice (2fN) for public benefit internet.

---

[i] Gyzal, R, 2011 ' The World's oldest writing", Online [Accessed April 29, 2-22] https://www.thenationalnews.com/uae/world-s-oldest-writing-not-poetry-but-a-shopping-receipt-1.568456

[ii] Dailey, A, "A brief history of receipts Abacus" Online: https://blog.abacus.com/a-brief-history-of-receipts-by-frank-addessi/ [Accessed April 29]

[iii] ISO/IEC 2011: 'Security Techniques Privacy Framework' Online https://www.iso.org/standard/45123.html

[iv] Lizar, M, Binns, R, 2012 "Call for Collaboration: Opening Up the Online Notice Infrastructure" Do Not Track and Beyond, online [accessed April 29]

[v] Kantara Initiative, 2022 Consent & Information Sharing WG, Consent Receipt v1.1 - Online [accessed April 29, 2022] https://kantarainitiative.org/download/7902/

[vi] ISO/IEC, 2020 '29184 Online privacy notice and consent' Online [accessed April 29, 2022] https://www.iso.org/standard/70331.html

- [vii] Note: SPECIAL project was funded to launch a W3C effort, by EU, this was co-launched with an event organized by the Kantara Consent Receipt work group at ODI headquarters in London. (co-located event with MIT Media labs.(ref).

[viii] W3C DPV, Data Privacy Vocabulary Control CG, Online [April 29, 2022] https://www.w3.org/community/dpvcg/

[ix] Cronk, J, 2017 Categories of Personal Information, https://enterprivacy.com/2017/03/01/categories-of-personal-information/

[x] Kantara Initiative, ANCR WG, ANCR-Record Specification v0.4, Online '[Accessed April 29, 2022] https://kantarainitiative.org/confluence/display/WA/ANCR+Record+v0.4

[xi] Convention 108 +, 2018, Council of Europe", Online [accessed April 2022] https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108

[xii] Controller Credential, Notice & Consent Task Force @ Trust over IPO, [accessed April 29,2022] https://wiki.trustoverip.org/pages/viewpage.action?pageId=76978