OPN: Open Notice Receipt Schema

Mark Lizar[1] and Harshvardhan J. Pandit[2]

[1] Open Consent Group Ltd - OPNUP@openconsent.com
[2] ADAPT Centre, Trinity College Dublin, Dublin, Ireland - pandith@tcd.ie

Abstract. Effective digital transparency largely depends on provision of a notice, which historically has been a static document such as a privacy policy rather than a contextually useful notice or sign. In this paper, we present Open Notice (OPN) network as a solution to address digital governance transparency challenges to make invisible changes to the state of policy (or governance) visible. OPN uses an open notice receipt schema to capture the semantics of a notice, which allows broadcasting changes and automating the tracking of policy changes.

Keywords: digital transparency, GDPR, privacy, privacy notice, schema

1 Introduction

A critical challenge for the trustworthiness of information sharing in today's internet-fuelled world is digital transparency. A key part of this challenge is the security and accountability of information sharing that is reliant upon regulations. For example, all privacy laws require a notice be provided to a person in order to manage the expectation of privacy (or governance). The information contained within online notices or signs is shaped by legal notice requirements that govern how privacy, surveillance, health, and safety are delivered.

Notices, the most common and interoperable privacy legal requirement[1], are intended to facilitate a shared understanding between provider and service consumers. In the context of shared understanding, notice is a broadly defined term, which includes terms of use, licenses, privacy policies and privacy statements. While approaches exist to express [7] and understand notifications through the use of a privacy policy [5,8], in the context of meaningful privacy or consent, transparency over the provenance of notice information is a key factor in assessing the compliance and security of the active state of governance a policy provides in context.

The lack of contextual transparency reflects an absence of the standardisation required for people to autonomously track changes to privacy[3], which presents a critical security and trust flaw with legacy notice infrastructure. This is also evident in the challenge of maintaining informed consent where a person is required to understand changes to a notice and for the provider to ensure people are sufficiently informed of such changes, without a record to automate transparency outside of the context of the notice.

2 Open Notice (OPN)

The OPN project originally started as an industry project in 2012 called Open Notice[6] that presented a call for standards collaboration to address the lack of governance transparency in online contexts. The objective was to address the global "fake policy notice/contract of adhesion" challenge that people experience when clicking a checkbox to agree to terms or policy they have not read and do not understand. OPN is a solution for the challenge to reverse the impossible burden of policy awareness placed on people is to improve upon the current experience for all stakeholders by reducing friction, improving the experience while also reducing the policy risk. OPN is available at `https://opn.openconsent.com/`.

The OPN Network, depicted in Fig 1, is used to maintain privacy profiles of a service provider and privacy processors to automate the tracking and broadcasting of policy states to people. The privacy profile of a controller is actively monitored so that changes can be tracked to provide an active privacy broadcasting signal. This signal is used to generate a notice receipt, which can be compared against the current (or future) state of privacy profile with the notice receipt schema. This enables the privacy network to provide a personalisation of privacy notices automatically and autonomously, which substantially reduces the repetitive burden to check notices requiring reading of policies in order to track unexpected changes in the state of policy.

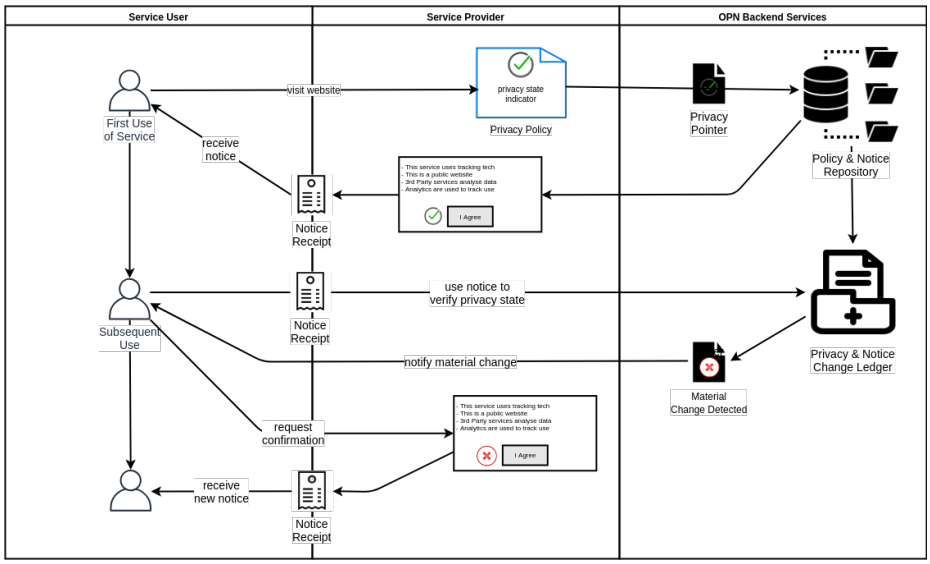

Fig. 1. Overview of OPN

In an OPN Network a public policy profile is generated when a provider (website or service) registers a policy pointer, a policy identity contact pointer (for example a Data Protection Officer), and a auto generated controller category policy profile statement in the network. Once this profile is published, the provider's profile is activated and verified, which is then automatically monitored for changes. The OPN Network stores changes to profile in a profile ledger so that changes can be annotated by the controller and broadcast automatically. People can generate a notice receipt on-demand (or automatically) for every context they interact with. The receipt is then used to check the provider profile for state changes, which once detected, is visualised using an icon embedded in the policy, e.g. by changing colour from green to red.

3 Notice Receipt Schema

The notice receipt schema consists of a set of fields used to define an interoperable receipt. The schema can be combined and used within other standards, such as JWT[3], to provide a single notice format that people can understand and use to control their own personal data utilising privacy rights, licenses and contracts. The schema can be represented using JSON-schema[4] or JSON-LD[5] to leverage its semantics with a web-native format. The notice receipt schema can be extended in different ways using different open standards and specifications such as ISO 29184[6], OASIS COEL[7], Kantara Consent Receipt [4], and W3C DPVCG[8]. Table. 1 provides an overview of the schema for the JSON specification with further documentation available online[9].

In the table, *label* denotes the field, *format* states the expected data type, and *req/opt* states if the field is required - where valid notice receipts MUST contain every field defined as required. The field *id* allows each receipt to be uniquely identified and referenced for provenance and compliance purposes. The field *timestamp* allows the receipt to be associated with a specific instance of policy state in time, and to detect future changes using the profile of the provider within the open notice network. The field *profile* allows the receipt to be compared with the latest state profile in ledger, and to notify the service user of any changes or updates. The identity of the provider is represented using the *controllerID* field in schema, with the term 'controller' used to align it with common international privacy legal vocabularies such as the GDPR.

The field *notice* links the receipt to the specific notice and information provided to the user, for example as an URL. The field *context* in the schema captures additional attributes about the provision of the notice such as the medium

[3] JSON Web Token `https://tools.ietf.org/html/rfc7519`
[4] JSON Schema `https://json-schema.org/`
[5] JSON-LD `https://json-ld.org/`
[6] ISO 29184 `https://www.iso.org/standard/70331.html`
[7] COEL `https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=coel`
[8] DPVCG `https://www.w3.org/community/dpvcg/`
[9] OPN Specification `https://openconsent.com/blog/2019/5/16/opn-receipt-spec`

Table 1. Notice Receipt Schema Fields (for JSON specification

label	format	description	req/opt
version	string	The version of specification used to which the receipt conforms. To refer to this version of the specification, the string "v1" or the IRI "https://w3id.org/OPN/v1" should be used.	req.
profile	string	Link to the controller's profile in the OPN registry.	req.
id	string	A unique number for each Notice Receipt. SHOULD use UUID-4 [RFC 4122].	req.
timestamp	integer	Date and time of when the notice was generated and provided. The JSON value MUST be expressed as the number of seconds since 1970-01-01 00:00:00 GMT (Unix epoch).	req.
key	string	The Controller's profile public key. Used to sign notice icons, receipts and policies for higher assurance.	opt.
language	string	Language in which the consent was obtained. MUST use ISO 639-1:2002 [ISO 639] if this field is used. Default is 'EN'.	opt.
controllerID	string	The identity (legal name) of the controller.	req.
jurisdiction	string	The jurisdiction(s) applicable to this notice	req.
controllerContact	string	Contact name of the Controller. Contact could be a telephone number or an email address or a twitter handle.	req.
notice	string	Link to the notice the receipt is for	opt.
policy	string	Link to the policies relevant to this notice e.g. privacy policy active at the time notice was provided	req.
context	string	Method of notice presentation, sign, website pop-up etc	opt.
justification	string	Authority of notice provider	opt.

it was provided in (e.g. online), or the method of presentation (e.g. pop-up dialogue). The field *jurisdiction* refers to applicable jurisdictions for assistance with legal compliance purposes. The policy applicable at the time of the provision of the notice is linked using the (*policy* field. Where such policies change over time, the link in the notice receipt should point to the correct specific version of the policy rather than the latest one. The field *justification* is used to capture information regarding authority of the notice provider.

Notice receipt providers can optionally provide a signing key or certificate using the field *key* to provide a higher assurance of non-repudiation for verification of the notice and the receipt. This verification key is generated when the provider of a notice registers their policy profile in the OPN Network profile registry. As the notice receipt schema itself does not contain any personally identifiable information, it is not constituted as personal data artefact. This allows the receipt to be safely shared with other services (by the service user) for purposes such as storage, verification of compliance, or extended automation

functionality. Within the OPN Network, each notice receipt is identified with a unique ID used to reference the COEL event atom [2] and stored in a 3rd party *COEL/Engine* for privacy compliance when the receipt is extended with personal data applications or standards.

4 Conclusion

A notice receipt is a demonstrable record of a service users consumption of a notice when it is provided by a service (e.g. website). The notice receipt is a machine readable record of the active 'state' of privacy, produced at the point of interaction, with a service in context. This notice captured 'state' can then be compared to future states to provide contextual transparency. OPN enables providers and consumers of notice to better track and understand the state of governance with automated machine readable governance contexts.

The notice receipt schema presented in this paper is central to the implementation of OPN Network to capture machine readable notice. Work is currently in progress to extend the combined schema with the Kantara Consent Receipt specification [4] and the DPVCG taxonomies[8] to add elements for a GDPR version of the Consent Receipt.

Acknowledgements

Harshvardhan J. Pandit is funded by the ADAPT Centre for Digital Content Technology which is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

References

1. Analysis of Privacy Principles: Making Privacy Operational (2007), http://xml.coverpages.org/ISTPA-AnalysisOfPrivacyPrinciplesV2.pdf
2. Classification of Everyday Living Version 1.0 (Jan 2019), https://docs.oasis-open.org/coel/COEL/v1.0/os/COEL-v1.0-os.pdf
3. Lizar, M., Potter, G.: Towards a framework of contextual integrity:legality, trust and compliance of CCTV signage. In: Doyle, A., Lippert, R.K., Lyon, D. (eds.) Eyes everywhere. Routledge, Abingdon (2012), http://eprints.lancs.ac.uk/74146/
4. Lizar, M., Turner, D.: Consent Receipt Specification v1.1.0. Tech. rep., Kantara Initiative (2017), https://docs.kantarainitiative.org/cis/consent-receipt-specification-v1-1-0.pdf
5. Oltramari, A., Piraviperumal, D., Schaub, F., Wilson, S., Cherivirala, S., Norton, T., Russell, N., Story, P., Reidenberg, J., Sadeh, N.: PrivOnto: A semantic framework for the analysis of privacy policies. Semantic Web **9**(2), 185–203 (Jan 2018). https://doi.org/10/gdfqnk, http://www.medra.org/servlet/aliasResolver?alias=iospress&doi=10.3233/SW-170283
6. Opening up the Online Notice Infrastructure An 'Open Notice' Call For Collaboration (2012), https://www.w3.org/2012/dnt-ws/position-papers/23.pdf
7. Schwartz, A.: Looking back at P3p: Lessons for the future. Center for Democracy & Technology, https://www. cdt. org/files/pdfs/P3P_Retro_Final_0. pdf (2009)
8. Terms of Service; Didn't Read, https://tosdr.org/