Transparency Performance Indicators – A User-Centric Methodology for Measuring the PII Controller Compliance and Conformance

# Abstract

Transparency, with regards to the purpose and justification, in the identification of personally identifiable information (PII) principals (individuals), is critical in order to manage security and privacy expectations. In order to achieve this PII Controllers must provide a notice that makes these risks evident. This is due to the fact PII Controllers must provide notice and information that can be used by the PII Principal to understand the risk and whether this is in line with their expectation for the use case and jurisdiction.

This is a problem largely unaddressed today online. Surveillance of individuals takes place without any knowledge of who is using and benefitting from personal information until it is too late to do anything about it. Attempts to address requirements for notice and consent substitute terms and conditions imposed on the PII Principal with little to no choice. User interfaces reinforce dark patterns where privacy and personal data control are minimized. There is a dire need for privacy and transparency technology, services and infrastructure to address these issue. This paper and presentation show a way forward leveraging human centric approaches to personal data control, legal requirements, and international identity, privacy, and security standards.

A notice which contains PII Controller information is a requirement across all security and privacy frameworks. At the Kantara Initiative Anchored Notice and Consent Receipt (ANCR) workgroup (WG), a methodology has been developed to measure PII Controller transparency and to map this to international standards and legal frameworks for security, privacy, notice, and consent. These include [ISO/IEC 29100:2024 Information Technology - Security Techniques - Privacy Framework](https://webstore.iec.ch/en/publication/92295), [ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements](https://www.iso.org/standard/27001) and [ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls](https://www.iso.org/standard/75652.html), [ISO/IEC TS 27560:2024 Privacy technologies — Consent record information structure](https://www.iso.org/standard/80392.html), [General Data Protection Regulation (GDPR)](https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng), and [CoE108+](https://www.coe.int/en/web/data-protection/convention108-and-protocol),

The four Transparency Performance Indicators (TPIs) consist of: 1. The timing of the notice identifying the Personally Identifiable Information (PII) Controller., 2. The content of the notice has all the compulsory information. 3. Access to, and usability of security and privacy rights explicit in the notice. 4. Proof of contextual cryptographic authority and security. These measures are taken to determine whether notice is adequate for any and all processing justifications, and in particular it looks to determine whether there is a valid basis for consent.

The paper also brings into use the concept and specification of notice and consent receipts. The Kantara Initiative published [Consent Receipt Specification Version 1.1.0](https://kantarainitiative.org/download/consent-receipt-specification/) which has been adopted by ISO in Annex B. of [ISO/IEC 291842020 Information technology — Online privacy notices and consent](https://www.iso.org/standard/70331.html) and also greatly influenced ISO/IEC 27650. The work and this paper present how a receipt can be used to capture the PII Controller notice and to make a record with it that can be used by the PII Principal, the PII Controller, and regulators.

These indicators measure the risk of (hidden) identification and tracking (surveillance) of the PII Principal. This represents a significant advancement toward decentralizing digital identification and surveillance governance. It does so with standards-based notice and consent records for proof of authority in online systems that map across identity, security, and privacy regulations.  Importantly, and in a divergence from ISO/IEC 27560 the record created using the TPIs does not require, and in fact make the strong point not to create, an identifier associated with the PII Principal.

The receipt and record capture the state of the relationship between the PII Principal and any downstream controller or record. It also allows the PII Principal to provide terms that govern the relationship and provide a legitimate basis for consent. The state of the relationship becomes the mutual expectation of governance in the processing of PII.

Examples are presented where the methodology is employed to look at the initiation of a browser session and the creation of cookies, and also for its use in a notice for a surveillance sign. In fact the PII Principal record acts like a “reverse cookie” in the sense that is used to identify and track the behavior of the PII Controller, whereas cookies are used to identify and track the behavior of the PII Principal.

Mapping legal requirements to the fields in the indicators and the resulting records allows the PII Principal to co-govern their activity online and in the physical world in coordination with security and privacy regulators. In addition to GDPR and CoE108+ the presentation also looks at [Quebec Law 25 Act Respecting the Protection of Personal Information in the Private Sector](https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1) and [The Personal Information Protection and Electronic Documents Act (PIPEDA)](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/) using the 11 privacy principles in ISO/IEC 29100:2024 which derive from Privacy by Design and before that from the [Fair Information Practice Principles (FIPPs).](https://www.fpc.gov/resources/fipps/)