Consent Receipts

Addressing the “biggest lies” which are:

consent & notice
What is a consent receipt?

A consent receipt does what it says on the tin. It tracks consent by making a record of it. (Similar to how a regular receipt is used to track money).
Agenda

• Background Of This Initiative

• Consent Receipts

• Open Notice Registry

• What’s next
Background

Some of the orgs supporting Open Notice

- "I have read and agree to the terms and conditions" - Biggest Lie on the web
- CommonTerms - One-screen summary of your terms
- customercommons.org
- Terms of Service Didn't Read - tosdr.org
- Usable Privacy Policy Project - usableprivacy.org

We fight the Biggest Lie. We meet on the OpenNotice.org maillist.
Notice needed for Consent

Without notice there is no consent:

“The most fundamental principle is notice.” (FTC, 1998)

“It is clear that a common mechanism to encode and publish the policies governing usage of services is needed.” (Internet Technical Advisory Committee, 2010)

Consent receipts fill the 'missing notice' gap
The Solution

• The open notice call for collaboration

• Joined Kantara Initiative Consent & Information Sharing (CIS) Work Group to develop specification standard for W3C

• Agreed a Standard format for consent notice would lay foundation for trusted services
Consent Receipt

• A common format for linking notice requirements into a usable format

• Focused on legal requirements for consent notices’

• Infrastructure that enables effective governance

• Opens the market for innovation in personal data control (A.K.A. Privacy)
Benefits of a Consent Receipt

• For **Individuals** (Knowledge & Control)
  • Consent management (before, during, and after)

• For **Companies** (Compliance & Trust)
  • Makes it easy (and cheap) for companies to comply with new laws

• For **Regulators** (Oversight & Management)
  • provides Regulators with flexibility to regulate and enforce regulations according to localised requirements

• For **Everyone**
  • Improving economic performance of policy solves many issues in identity management
Economic Performance of Notice & Consent

• Est. infrastructure costs exceed £3.3bn a year at this time

  • £1.65 billion inside organisations and another £1.65 billion of consumers’ time costs

• Evolving consumer data control and policy usability is estimated to reduce these costs by 96% in the UK over next 10 years bringing costs down to £150 million a year

• Enabling “Economics of Identity” UK Whitepaper by Ctrl Shift (www.ctrl-shift.co.uk)
Implementation of Consent Receipts

- Starting with a Minimum Viable Consent Receipt (for online transactions)
  - Compliance By Default framework
- Exponential Interoperability between jurisdictions and industries
  - Extensible by jurisdiction, industry, sensitivity of data, context (data origin),
    - E.g. Health Care legal notice requirements can be added for sensitive medical data
- Further extended by another jurisdictions notice requirements for cross border transfer or sensitive personal data
Trust Delivery System

- Interoperability starts by combining trust services in context

- A **consent receipt** is a vehicle for trusted services,

- Icons and assurance frameworks can be added in the consent receipt to serve advanced compliance requirements
Open Notice Registry

- Provides public foundation for a two-way communication between people and organisations on policy/terms.

- An Open Notice Registry (similar to the ICO data controller registry) is the database behind the receipt.

- Used for companies to register their notice and provide consent receipts to people.

- Providing an independent channel for interaction.
Co-Regulation & Self-Regulation

- A consent receipt is like a transaction receipt
- Everyone gets the same transparency, and provides a framework self regulation

- **Open Notice Registry + Consent Receipt = Co-regulation**
- Minimise the need for regulator enforcement,
- Evolve further the ICO Governance Frameworks
UK- Information Commissioner Assurance Scale

<table>
<thead>
<tr>
<th>Colour code</th>
<th>Internal audit opinion</th>
<th>Recommendation priority</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High assurance</td>
<td>Minor points only are likely to be raised</td>
<td>There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non compliance with the DPA.</td>
</tr>
<tr>
<td></td>
<td>Reasonable assurance</td>
<td>Low priority</td>
<td>There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.</td>
</tr>
<tr>
<td></td>
<td>Limited assurance</td>
<td>Medium priority</td>
<td>There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.</td>
</tr>
<tr>
<td></td>
<td>Very limited assurance</td>
<td>High priority</td>
<td>There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.</td>
</tr>
</tbody>
</table>

http://ico.org.uk/for_organisations/
A Measure of Compliance

- A consent without notice or basic notices requirements like contact information or policy information.
- More generally notices that incorrectly describe choice and purpose.
- Organisation that meet notice requirements.
- Exceeds compliance requirements.
- ICO Promise, Audited, Use third party trusted services frameworks.
<table>
<thead>
<tr>
<th>Notice Compliance Checklist</th>
<th>Non</th>
<th>Partially compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>contact</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>purpose</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>consent notice information</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3rd party Listed</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Simple Consent Notice Compliance
What’s Next: How?

• Developing a community for trusted services

• Developing an Alpha Open Notice Registry for orgs that want to self assert and provide consent receipts

• Research with MIT Media Labs this summer on asserting data control by people.
  • Estimate 90% + of orgs are not aware or able to comply to requests about notice. We want to test this estimate.

• Many ways to develop further, many are in reaction to the ICO
  • A consent receipt in a browser extension or a web service will enable people to self-provide a framework to hold privacy icons.
  • A plugin can enable automated creation of an open policy registrar

• Consent Receipt Request: Status of consent - Won hackathon in FEb
Thank You

Mark Lizar & John Wunderlich
hello@opennotice.org
References


“The Origins of Personal Data and its Implications for Governance”


How Good is Trust?
Adolfo Morrone1, Noemi Tontoranelli2, Giulia Ranuzzi3 Measuring Trust and its Role for the Progress of Societies

Economics of Identity - > https://www.ctrl-shift.co.uk/research/product/89