Kantara CISWG: Consent Receipt Specification

In response to Notice of Consultation and Call for Essays: Office of the **Privacy Commissioner** of Canada,

We are writing to you on behalf of the Consent and Information Sharing Work Group (CISWG) at the Kantara Initiative.

We are happy to update the Privacy Commissioner on the consent receipt project.   Essentially, a format for recording consent and providing a consent receipt to people. Much like receipts are provided to people when they purchase something in a store.

Intended to open personal data control for people through consent and information sharing transparency. Laying the foundation for improving the control and by extension experience people have when providing consent and sharing personal information.

We aim to have a V.1 Consent Receipt specification in September 2016.

Kind Regards,

Signed:
Mark Lizar Co-Chair CISWG
Iain Henderson Co-Chair CISWG

Introduction

The consent receipt is a cross cutting, horizontal specification that is quite similar in many ways to, the concept of a receipt for purchase of goods and services.

Background

The idea of a receipt for the trade of goods and services is not a new idea. In fact the oldest form of writing is not a poem or a story but a receipt.[1] The first receipt was an indicator of a new level of accounting for goods and services in which abstract accounting of goods and services was used to create trust, control and confidence in the trade of goods and services.

Throughout history, accounting provides a great example of how transparency has developed so that people can track the sharing of things they can't see. In many ways, accounting for money before receipts is like trying to track personal data without recording how and who its shared with today.

People would see one price on the shelf and get a more expensive one at the register. Today people consent to a policy and share personal information and the policy can change as soon as the service is used. There are often over riding data sharing agreements between domains that are not transparent. The burden of understanding these multiple policies and their consequences is pushed on the individual.

Before receipts were added to registers, a bell was a visceral noticed that rang when a cash register drawer was opened. Notifying that money was exchanging hands, receipts were then written. Eventually, accounting and commerce were combined so that receipts are generated by the transaction event. Similarly, people can't track consent to personal data processing unless they do it them selves one consent at a time, but ask someone what they agreed to last week and what their personal information sharing practices are at any one time and it would very difficult if not impossible for an individual to comply.

At this time the Consent Receipt is the only international standard candidate for accounting for the use and control of personal information via consent. In fact, there is no practice of providing a record of consent, yet every OECD FIPPs based jurisdiction has regulation based on an openness principle. PIPEDA Principle 8, is Openness, as a result this paper is put forward with the claim that currently personal data and consent is not open enough to include people.

---

[1] Ghazel, Rym, 2011 " World's oldest writing not poetry but a shopping receipt" The National {online: last accessed May 2016} http://www.thenational.ae/news/uae-

Openness

The (PIPEDA) principle of **Openness** states that an organization shall make its policies and procedures about how it manages personal information readily available.

Advice online goes on to further advise that:

An Organisation should not provide barriers to access — if an individual is making a request to know about your organization's information handling practices, the request should be done without an unreasonable effort

When providing the information, it should be available in a form that's generally understandable. The information should be provided in plain, simple English that someone without a university degree can understand — save legalese for your lawyers and contracts.

Its clear now, with the digital information sharing practices that have developed over the last two decades, that this level of Openness is not enough. It leaves the individual out of the loop, unable to manage and understand consent and information sharing practices as a whole.

Consent and notice infrastructure has barely evolved at all in the last 20 years.   The policies and consent practices today place an unfair burden on people. Requiring people to read, track and understand policies, which due to their sheer detail, render people unable to track personal information sharing once they click I accept.

Economics of personal information

"As our personal information becomes increasingly monetized and serves as a new form of currency that drives our new digital economy, the incentive to collect and use it for new innovative purposes can barely be contained. Every day there are new, creative ideas on how businesses can derive more profit from our personal information and whole new business models are redefining our concept of commercial activity. "[2]

A common consent record, provides people with ability to manage consent on aggregate outside of the siloed company context in a much more experiential and meaningful manner.   A consent receipt inherently (by being a receipt) provides transparency over consent and

---

[2] 2015, "OPC Strategic Priorities 2015-2020" [Online] https://www.priv.gc.ca/information/pub/pp_2015_e.pdf

information sharing practices and can be used to track service providers and reputation. Enabling an open market in personal information management services.

Already, there are many personal agent technologies being developed to provide the service architecture for people to harness the power of their own data.

The consent receipt specification is the anchor for the development of consent framework for people to see how to authorise themselves, control their own persona, create their own loyalties.

Dynamic Consent & Trust

The Kantara Initiative: Consent & Information Sharing workgroup have been working on developing 'Consent Receipts v1" with an ambitious objective of having a v1 CR spec for September 2016.

The consent receipt effort began in 2012 and evolved into a specification which, is just now getting close to a Kantara Initiative community review so it can be released publically.

> "A first goal for the OPC will be to enhance the privacy protection and trust of individuals so that they may confidently participate in an innovative digital economy."[3]

The *economics* of personal information extend to discussion of what is the social, legal, and commercial transparency over consent.

Unlike a paper receipt, a consent receipt also has the qualities of a digital record, like a web cookie. In some respects, a consent receipt, could be described as a reverse cookie, in that, the individual and the organisation both have a record of the consent, and the individual can use it to track and profile the organisation and/or service along with consent and information sharing preferences. Thus, the playing field is levelled, people can track sharing with 3rd parties, like 3rd parties can track people.   Enabling people to use consent receipts to communicate with the data controllers and of course withdraw consent. As specified in recently published European Regulation[4] (making digital consent dynamic)

The beta version v0.8 of the Consent Receipt Specification will be available in late May, and, at this time we would like to propose that Canada take a lead in generating consent transparency and opening personal data control by advocating and supporting the use of consent receipts. Canada is a nation with an identity that is proud of freedom, privacy, and quality of life openness affords Canadian citizens.

---

[3] 2015, "OPC Strategic Prioritiees 2015-2020" [Online]
https://www.priv.gc.ca/information/pub/pp_2015_e.pdf
[4] May 4th "General Data Protection Regulation" (2016) http://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

The simplicity of the Canadian privacy law provide an ideal environment for the consent receipt. Providing a tool for transparency, to enable people to see and manage their data sharing practices.

> "Protecting Canadians in a Borderless World In a globally networked and integrated economy, personal information and data can move quickly and effortlessly around the globe, including in countries that have weak privacy protections or none at all, potentially compromising the privacy of Canadians abroad. How can we effectively protect personal data flows in a virtual world that knows no checks or borders? "[5]

Protection of personal data across boarders is a very popular topic this year with the failure of EU Safe Harbour agreement with the US. The new Privacy Shield adds additional safeguards for the protection of Europeans data. This includes, but not limited too, stipulations for 3rd party sharing to be specified, with contracts, and protocols for redress.[6]

The consent and information sharing receipt has an entire section devoted to specifying 3rd party sharing, 3rd party purpose, sharing termination and the technical and legal scopes which accompany these sharing practices.

Reputation

The Consent Receipt specifications core focus is to provide a communication channel between people and services about consent and information sharing.

This makes a CR an ideal vehicle and context for standards, reputation, kitemarks and trust applications . An area of trusted services. Services that are represented by privacy icons, trust marks, protocols, personal agents, and personal information management services and industry best practices. All initiatives, which themselves audit practices and vet organisations in order to monitor trusted practices.

Similar to how people could not easily see if they are being deceived at the cash register, without a consent receipt, policies change and people are not able to manage their consent and information, or maintain meaningful consent without being able to track sharing themselves.

Without detailed sharing specification, contracts between parties, over sight and transparency, protecting a Canadian's personal information once outside of Canada is almost impossible.

---

[5] Ibid.
[6] Privacy Shield Annex [Online] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf

Specification Details

The current version and status of the sepcfication can be found on the Kantara Initiative Wiki[7]
The terminology and field selection has been determined by existing principles, law, best pratices and the ISO 29100 privacy framework. We also have elements and definitions in the specification that are best of breed from various jurisidictions.

The consent receipt is conceptualised from a human centric point of view.   In this regard the consent receipt v.1 for online is broken down into 6 sections.

1. Header

This has the information needed to use the consetn receipt on aggregate and for both parties to prove consent.

Field #	Field Name	Open Consent: Receipt v0.7	Consent Receipt v1	Sensitive v2	COMPLIANT v2.1
1	*Jurisdiction*	SHOULD	MUST	MUST	MUST
2	*Consent Time Stamp*	MUST	MUST	MUST	MUST
3	*Collection Method*	SHOULD	MAY	MUST	MUST
4	*Consent ID*	SHOULD	MUST	MUST	MUST
5	*PI Principal ID*	MUST	MUST	MUST	MUST

2. Data Controller Information

The identity and trust attributes of the Data Controller. These include address, location, privacy policy, and importantly contact information that is proportional to the context.

Field #	Field Name	Open Consent: Receipt v0.7	Consent Receipt v1	Sensitive v2	COMPLIANT v2.1
7	*PI Controller*	MUST	MUST	MUST	MUST
8	*On Behalf*	MUST	MUST	MUST	MUST
9	*Contact Name*	SHOULD	SHOULD	SHOULD	SHOULD
10	*Contact Address*	MUST 1 of 9-13	SHOULD	MUST	SHOULD
11	*Contact Email*	MUST 1 of 9-13	MUST	SHOULD	SHOULD
12	*Contact Phone*	MUST 1 of 9-13	SHOULD	MUST	SHOULD

---

[7] Kantara CISWG: Consent Receipt WIKI Page [Online]
"https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specificati on?src=contextnavchildm ode

13	*Contact Other*	MUST 1 of 9-13	OPTIONAL	OPTIONAL	OPTIONAL
14	*Privacy Policy*	MUST	MUST	MUST	MUST

3. Purpose Specification

These are the details, which are specified depending on the context, and context of use.   The reason and scope of personal data processing should be apparent, and icon sets for purpose and attributes are intended to be used in receipts to provide a click receipt function to the individual , rather that a policy reference.

Field #	Field Name	Open Consent: Receipt v0.7	Consent Receipt v1	Sensitive v2	COMPLIANT v2.1
15	Service	SHOULD	MUST	MUST	MUST
16	Link to Purpose	OPTIONAL	OPTIONAL	MUST	MUST
17	Purpose Category	SHOULD	MUST	MUST	N/A
18	*Consent Type*	SHOULD	MUST	MUST	MUST
19	Purpose Preference (Y/N)	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL
20	Purpose Termination/Duration/Renewal	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL

4. Personal Information Categories and descriptions
The PI Category is used to specify the type of PI that is collected and process.

Field #	Field Name	Open Consent: Receipt v0.7	Consent Receipt v1	Sensitive v2	COMPLIANT v2.1
21	PI Category	MUST	MUST	MUST	MUST
22	PI Sharing Y/N	SHOULD	MUST	MUST	MUST

5. Sharing

Field #	Field Name	Open Consent: Receipt v0.7	Consent Receipt v1	Sensitive v2	COMPLIANT v2.1
22	PI Sharing Y/N	SHOULD	MUST	MUST	MUST
23	Third Party	SHOULD	SHOULD	SHOULD	SHOULD

6. Scopes

Field #	Field Name	Open Consent: Receipt v0.7	Consent Receipt v1	Sensitiv
24	Scope(s)	OPTIONAL	OPTIONAL	MUST

The technical and functional scopes can be captured during the consent receipt creation and often change and develop iteratively with the use of consent.

If the scope of use changes significantly than a new consent is required.

The advanced v.2 CR specification will add a few more fields, for specifying sensitive personal data, for delegation of consent authority, 3rd party contract, termination and tracking.   In addition, we will be illustrating compliance with specific regulations by adding trust frameworks for terms and conditions to receipts.

Road Map: 2016-2018

Milestone	2016	2017	2018
V.0.8	June 1		
Summer Alpha Pilot	June 1		
V.1	September		
Interoperability & Conformance Dev		Whole Year	
V.2 - ISO 29100 -map laws and technical scopes			Jan

For more information
(note

Kantarainitiative.org
CISWG: Wiki
Consentreciept.org
http://real-consent.org

Spec Dev/Demo Materials
V0.7 Generator: https://api.consentreciept.org
V0.7 Generator Doc: https://api.consentreciept.org/doc
        -