Aug 5, 2016 * rev Aug 18 *

Open Consent: Scalable and Balanced Governance

Globalised Co-Regulation for Balancing Market Self-Regulation

Authors: Mark Lizar[1], Antti Poikola & Harri Honko, Katryna Dow & Nathan Kinch, Joss Langford, Michele Nati

** Mark Lizar - Open Consent CIC & Kantara Initiative: Co-Chair of Consent & Information Sharing WG
** Antti Poikola & Harri Honko - MyData Finland
** Michele Nati - Digital Catapult: Personal Data & Trust Network
** Joss Langford - Coelition
** Katryna Dow & Nathan Kinch - Meeco

This submission is in response to: Notice of Consultation and Call for Submissions, which is based upon the Consent Discussion Paper 'exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act' (PIPEDA)

[1] Corresponding Author - Mark Lizar - * mark@openconsent.org +44 (0) 2081232476

Open Consent: For Personal Data & Trust of My Data

About this Submission

This submission has been curated by a Canadian from Toronto, Ontario[2], who believes, "If you can't see how your personal data is being used, or who it is shared with, you are not free to share and trust in today's digital society."[3] This is echoed by the OECD/Berkman paper, "Law and technology must be crafted to respect certain "Properties of Identity" in order for the information society to be free and open."[4] In that respect, these properties should naturally be controlled by the people.

Most importantly, this sentiment is shared by a growing number of communities, services, and products internationally, which are represented by the organisations who champion this

[2] Ibid .1 also CEO of Smart Species Ltd Canada.
[3] Ibid. 1
[4] Rundle, M., Blakley, B., Nadalin, A., Seltzer, W., et al.
2007. "At A CROSSROADS: 'PERSONHOOD AND DIGITAL IDENTITY IN THE INFORMATION SOCIETY" OECD & Berkman Cyber Law Centre [July 2016] https://cyber.law.harvard.edu/node/94199

submission: MyData Finland, Digital Catapult: Personal Data & Trust Network, The Kantara Initiative, Coelition's Trust Ecosystem, and Meeco's Personal Life Management platform.

Submission Requirements:

1. You must state that you have read and understood these consultation procedures.
   - *We have read and understood the consultation procedures.*
2. Your submission must answer one (or more) of the four questions posed in the consent paper.
   - *We have addressed the 4 questions, and broadly and specifically answered the questions about consent governance as explicitly referenced in the consultation.*
3. You should clearly indicate which actor(s) (for example, industry, regulators, government) your comments are meant to implicate.
   - *The actors are clearly referenced in the background of this submission.*

Table of Contents

***** Excellent Quotes explored from the OPC discussion paper *****

"Such exceptions recognize that individual consent, and the autonomy it protects, do not override all other interests, but rather that there needs to be a balance between privacy and competing values which individual consent might undermine."[5]

"Consent should not be a burden for either individuals or organizations, nor should it pose a barrier to innovation and to the benefits of technological developments to individuals, organizations and society. But how do we best preserve this important control given the current landscape and achieve a balance between the individual's right to privacy and the organization's need to manage personal information for reasonable business purposes, furthering the very purpose and objectives of PIPEDA? What tools would be effective and who is best placed to implement them? "[6]

Summary

The Consent and privacy discussion paper the Officer of the Privacy Commissioner (OPC) presented, is intended to explore enhancements to PIPEDA and summarises 'Human Behaviour' as a challenge to meaningful consent. As,"paradoxes of human behaviour and the practical realities of having limited time and energy to fully engage with privacy policies."[7] For example, parents concerned about their children's privacy, do not have the time to read privacy policies and appropriately protect the autonomy of their children.

To address these concerns, the Open Consent, Consent Tech Framework, which is presented in this response, is being designed to empower people to make consent choices independently, beyond the initial point of consent. And by using open standards, make interoperable these independent choices enabling meaningful consent with powerful tools of consent management, which can be used to aggregate consent to manage multiple consents at once.

The current model of consent does not provide a meaningful model for consent management out of the initial consent context and therefore limits what can be construed as informed and "usable consent."[8]

In this submission we refer to some outstanding projects developing in the global personal data ecosystem, which illustrate the value of interoperability through the use of a common standards for consent.

[5] Ibid. 2
[6] Ibid. 2
[7] Ibid. 2
[8] Lizar, M,. Hodder, M,. 2014 "Usable consents: tracking and managing use of personal data with a consent transaction receipt" Published by ACM [July 2016] http://dl.acm.org/citation.cfm?id=2641681

We understand that enabling people with usable and meaningful consent is empowering and has an immediate impact on trust, individual autonomy and in effect digital society. While we also understand that consent is not a panacea for all issues presented in the discussion paper provided by Office of the Privacy Commissioner of Canada (OPC).[9] First and foremost, we are advocating "[a]n approach to privacy laws that does not reject notice and choice, but does not seek to rely on it for all purposes."[10] There is a strong role for ethics, enhanced accountability and clear boundaries in the use of data. Ethics need to be clear, enforced, transparent and provided in a way so that people have easy and even automatic access to consent withdrawal and redress when needed.

The Open Consent Framework (OCF), that we advocate, is designed with the premise of making consent transparent on scale, across jurisdictions, domains and the Internet. The consent framework utilises an open standard candidate called a consent receipt,[11] which provides records of consent that can be aggregated to show an overall picture of personal consents provided and information sharing.

Once transparency over data control is achieved and people are able to manage consent holistically, there will be more control and trust in the way people share information and trust, enabling people to explicitly assert preferences, attributes, and manage pseudonymity from a trusted notice, consent and privacy framework.

In response to the call to explore the potential enhancements to consent under PIPEDA, we aim to provide an overview of the emerging effort to develop Open Consent. Not only as an enabler for a global baseline for personal data & trust policy, across domains, or as a framework to provide systemic transparency over consent, but, as an opportunity for Canada to leverage its world class PIPEDA privacy legal framework. Taking the lead to enable Canadians with next generation consent based innovation.

Background

The OPC's call for an exploration into consent is well timed, as it coincides with the adoption of a standard consent specification for transparency over consent compliance, from which this response is based.

---

[9] Ibid. 2

[10] Cate, F., 2006 "Consumer Protection in the Age of the Information Economy" [July 2016] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972

[11] Lizar, M., "Kantara CISWG: Consent Receipt Specification" to the OPC May 5th, 2016 (https://kantarainitiative.org/confluence/download/attachments/76447870/CISWGCanadaSub.v.3.Final.pd) [Accessed July 20, 2016]

MyData, as defined by the Nordic MyData project,[12] 'is personal data whose use or access the individual human controls'.

As mentioned in the discussion paper, a mix of solutions are required, and a "balance between individuals right to privacy and the organisation's need to manage personal information for reasonable business purposes"[13] is required.

The Finnish MyData project[14] and the UK Digital Catapult: Personal Data & Trust Network[15] illustrate a cutting edge approach by government to enable personal data control. Meeco, a life management platform,[16] is used by people to explicitly consent to sharing information on a granular level. Coelition, based on the COEL standard,[17] developed in the standards community OASIS[18], provides a trust ecosystem for pseudonymisation of the collection and use of behaviour data at scale for big data and IoT environments, covering the spectrum of consent in the ecosystem.

A key challenge, which has been preventing the evolution of a global consent architecture online (and offline), has been the closed bespoke implementation of privacy policies that lack the inclusion of the people providing consent. Historically, this makes sense. Organizations and governments have been responsible for managing all the data and terms of agreements people make when sharing information.

In response to this historical challenge with personal data control, the risks and the economic benefits are clear. "Innovation economists estimate that the output and productivity of firms that adopt personal data-driven decision making are 5-6% higher than would be expected from other investments in information sharing technology", and provides an 8% advantage over competition.[19] In this regard, the barriers related to sharing closed and proprietary (including personal) data and associated privacy and trust issues hinder the opportunities to harness the value from data as a way of boosting economic productivity domestically and illustrate key opportunities in taking the lead with first-mover advantage in these areas internationally.[20]

---

[12] MyData Finland, 2014 "A Nordic Model for human-centered personal data management and processing", http://www.lvm.fi/en/-/mydata-a-nordic-model-for-human-centered-personal-data-management-and-processing-860616

[13] Ibid. 2

[14] Ibid. 12

[15] Digital Catapult,. 2015 "Personal Data & Trust Network" [July 2016] https://pdtn.org/

[16] Meeco,. "Life Management Platform" [2016] https://meeco.me/

[17] Classification of Everyday Living Technical Committee https://www.oasis-open.org/committees/coel/

[18] OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. https://www.oasis-open.org/org

[19] Brynjolfsson, Erik et al. 2011 "Strength in numbers: How does data-driven decision making affect firm performance?" ssrn.com. As of 10 Sept 2015: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486

[20] World Economic Forum, 2013 "Unlocking the value of Personal Data, form the Collection to Usage" weforum.org. As of 10 September 2015.

This aligns with the European Commission's Big Data Strategy for closed data and personal data sharing. The UK internet-based economy will represent 12.4 % of the UK GDP in 2016, and the global opportunity for the industrial Internet of Things is estimated to be worth 14.2 Trillion Euros by 2030[21]. In terms of personal data, Boston Consulting Group estimated the market's economic value of consumers' data at €1 trillion by 2020 across the EU.[22] Similarly Nesta estimated the new class of Personal Information Management Systems (PIMS) to have a market opportunity of £16.5bn in the UK.[23]

Introduction

In the past, people were not able to keep a record of their own consent, and they were not able to see or manage consent on aggregate, independently of the organisations providing people with information-reliant services. As a result, it has been very difficult for people to get a "clear understanding of what will be collected, how their personal information will be used, and with whom it will be shared."[24]

In particular, the explicit sharing, control, and trust in the use of personal information is the subject of intense debate and concern at this time.

The consent discussion paper presented by the OPC recognises the limitation to the current consent-harvesting model and the growing complexity of distributed data collection and processing, where "binary one-time consent is being increasingly challenged because it reflects a decision at a moment in time, under specific circumstances, and is tied to the original context for the decision, whereas that is not how many business models and technologies work anymore."[25]

In addition, big data, artificial intelligence, and behavioural event-based analysis reveal deep insights into people, their lives, and their families. Algorithms and analytics, which are opaque, provide increasing risk to people and rewards for companies in today's society.

---

http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

[21] Accenture. 2014. "Driving Unconventional Growth through the Industrial Internet of Things.' Accenture.com [Sept 2015] https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIot.pdf

[22] Rose, J. et al. 2012. "The Value of our Digital Identity" bcgperspectives.com [July 2016] https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/

[23] Nesta, 2014. "How to make £16.5 bn by protecting personal data.' nesta.org [Sept 2015] https://www.nesta.org.uk/blog/how-make-ps165bn-protecting-personal-data

[24] Ibid. 2

[25] Ibid. 2

Feeding big data and its subsequent analytics, and the incredible proliferation of IoT devices, is the clear awareness from regulators that this will challenge the notion of consent as it is currently defined in Canadian and international regulation.

To address these concerns, a much more holistic approach, based upon the Kantara Consent Receipt Specification candidate,[26] is being developed in the Kantara Initiative. Also, there are other standards drafts in work, like that of the ISO guidelines for Online Notice and Consent[27], which amongst other worthy goals is being fast tracked as a way to develop a bridge from the Kantara specification and the ISO 29100 Privacy framework.[28]

What is Open Consent?	What is Closed Consent?
Consent can be opened by providing people with access to a record of consent, at the point of consent, so that people can independently manage consent themselves and exercise personal data control. Open consent is the practice of including people in consent transactions by providing people a record of their consent at the point consent is provided.	Currently, people provide consent but have no way to keep a record of what consent they have provided, to whom, and for what reasons. This closed consent architecture, which is globally in place on the Internet today, prevents people from tracking and learning from the choices they have made, and how their information is shared and used.

Open Consent to Create 'Real Consent'

The Open Consent project has been developing through a series of 'Real Consent' workshops, research, and events produced by a collaboration facilitated by Digital Catapult's Personal Data & Trust Network and sponsored by the Kantara Initiative.

---

[26] Kantara Consent & Information Sharing WG, 2016 (in progress) "Consent Receipt Specification v0.8" [July 2016] https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification?src=contextnavchildmode

[27] ISO, IEC/AWI, 29184, (in progress). "Guidelines for Online Privacy Notices and Consent" iso.org [July 2016] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=70331

[28] ISO, ISO/IEC, 29100, 2011. "Information Technology -- Security Techniques -- Privacy Framework" iso.org [July 2016] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

The first event, 'Assess the Gap'(Jan 28th Privacy Day) was the result of an MIT Media Labs 'Future Commerce' UnConference and Hackathon[29], which was intended to ascertain the state of play with the Personal Data Trust Network at Digital Catapult and create a plan to make Real Consent. It was a Personal Data and Trust network initiative to research and assess the market gap to consent compliance.

The second event, 'Consent By Design' (March 21, 2016), focused on both the experience of consent and the economic model for consent for information sharing. This event was produced in conjunction with Alessandro Carelli, a PhD student from Loughborough University, who engineered a consent-by-design template, which was used to examine the consent experience for the workshop in order to develop the concept of an open consent for the Digital Catapult space we were having the event in.

The third event, 'Real Consent & A look @ Trust' (May 27, 2016), was a master class of consent expertise from in- and outside of the Personal Data & Trust Networks, in which the Open Consent Framework was first discussed as a functional approach. This inspired Digital Catapult to take the lead by implementing the first physical digital consent space consent receipt, live in London from Sept 1, 2016.

The fourth event, Open Consent for Real Consent (will be held on Sept 26th 2016), is where the results of the prototyping and alpha testing will be reviewed, and a presentation of the work, with invitations for greater engagement at an international level, will be delivered. (To get involved join the personal data network at http://pdtn.org.)

The fifth and final event (Date TBA) will signal the end of the one year challenge to produce Real Consent that started at the MIT Future Commerce Hackathon. In this last event, the report and/or output of the Real Consent project will be provided. First, the effectiveness of Open Consent to achieve Real Consent will be presented and discussed, and following that, there will be a focus on what would be required to make Real Consent sustainable and operational at a global scale.

Open Consent (so far)

At this stage of the Real Consent project Digital Catapult is integrating consent receipts into its front-of-house concierge systems at its London office and event space (normally attended by 1200 external visitors every month, not including event attendees) in order to test end-user acceptance for the consent receipt and measure its impact as a tool for transparency and end-user control. The initial output of this consent receipt implementation is to measure the generation of trust through greater transparency and data control over the way organizations collect and (eventually) disclose personal data.

[29]Greenwood, D,. "Future Commerce Hackathon and Unconference", [Online July 2016] https://sap.mit.edu/media-lab/event/futurecommerce-hackathon-symposium

Trials are expected to be performed in the fall 2016. At the same time Digital Catapult is user testing the consent receipt.

With a successful outcome, the objective of facilitating adoption and use of the consent receipt as a tool to demonstrate basic compliance with current laws globally can be reported.

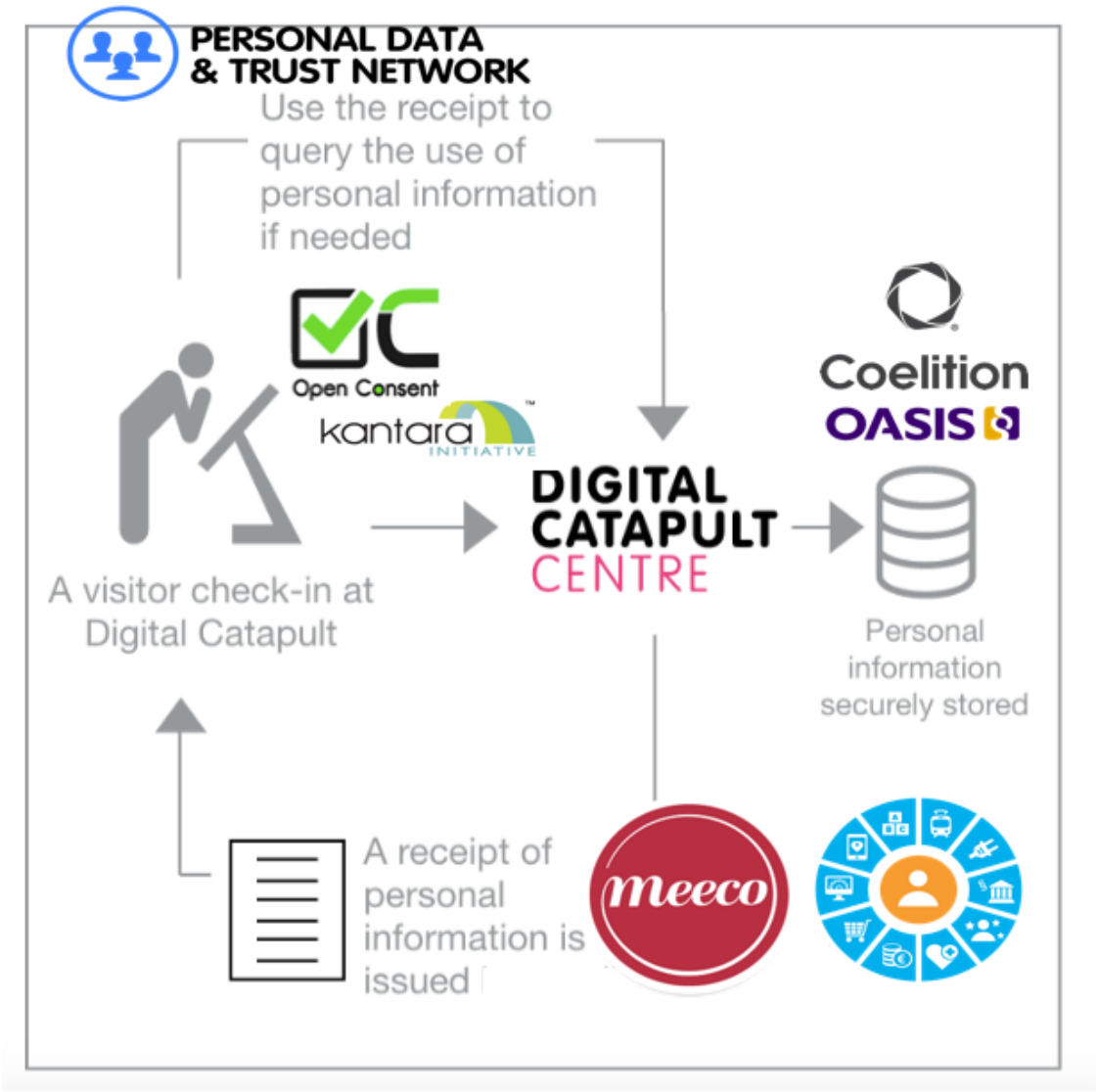
The next level of consent tech hacking will be in the MyData led UltraHack 2016 competition in Helsinki on Aug 29th.

The second stage of this Digital Catapult sponsored project will feed the results of these activities, and the sharing of lessons learned, into the open consent framework discussion, with an Does Open Consent make Real Consent? event, on Sept 26, 2016, hosted at Digital Catapult.

With the ultimate aim of promoting good practice and innovation in Personal Data and Trust.

For Example:

An illustration of function amongst participants in 2016



- In this illustration, Personal Data & Trust Network members, when visiting Digital Catapult, sign in to the concierge system and receive an improved customer consent experience. An experience that also makes transparent, compliance with European, UK, US Canadian privacy notice requirements with a consent receitpt. A receipt which streamlines consent management for people.
- People are issued with a standardized consent receipt developed with the assurance of the Open Consent Framework and the interoperability of the Kantara Initiative's consent receipt specification.
- The consent receipt provides people with transparency over the way Digital Catapult collect and treat their personal data and who it is shared with. Making people more

comfortable sharing when participating in a space of innovation streamlining the consent experience.

- In addition, the consent receipt provides transparency after consent is provided enabling PDT members to track the data they share and easily revoke their consent to Digital Catapult to use this data.
- Consent receipts are generated by a privacy preserving architecture, using standardized pseudonymous tools, exemplified by Coelition IDA, that protect the unlinkability between users.
- Consent specification is being developed to work with User Managed Access
- As more and more personal data and trust member's services adopt the consent receipt as a standardized and interoperable tool for personal data, a growing network of trust will emerge.
- By presenting compliant, trustworthy and privacy preserving infrastructure using the OCF we envision that an ecosystem of new and compliant personal data services, in control of the individual, will be developed.
- To demonstrate the potential of the specification to support cross domain validation, service non-repudiation, and most importantly multi jurisdictional harmonisation, it takes a community of communities to have a single vision to make real change.

- [Note: In this example, this diagram above is a parody of the actual Digital Catapult implementation of the digital catapult consent receipt for the physical Digital Catapult space, by including the technology and infrastructures of the wider ecosystem represented by the authors of this paper who are collaborating to make this happen in 2016.]

As illustrated in the above example, Open Consent is used as a framework of transparency for people, establishing a common open consent notice practice that enables people and organisations to aggregate, track, and easily manage their own consent and in effect personal data control. A key function of this practice is to foster the open practice of being able to manage consent past the point of the one time, closed consent bottleneck, which is what is experienced today.

To this end, Open Consent has been conceived to provide the foundation for common consent management controls that enable people to share information explicitly and companies to provide proof of consent.

Efforts described below, like UMA, Meeco and Coelition, are representative of a growing segment of consent technologies, communities and governments, driving the personal data ecosystem so that people can themselves have meaningful personal data control.

Governance: Market Self-Regulation

Governance Questions Presented for Exploration[30]

a) Codes of practice Questions

1. Could sectoral codes of practice indeed enhance consent and/or privacy protection?
2. How would they be enforceable?
3. Who should be involved in developing sectoral codes? Who should be responsible for overseeing compliance with sectoral codes?

b) Privacy Trustmarks Questions

1. Under what conditions are trustmarks a sensible and reliable tool for protecting consumer privacy in the evolving digital environment?
2. How would a privacy seal program work alongside PIPEDA?

Using a common and standardized consent receipt, is just a piece, albeit the founding piece, of building a globally interoperable and scalable infrastructure for governance that scales across jurisdictions.

An open standard for a common consent record requires an open consent and information sharing assessment in order to create a consistent consent record template, as well as a trustworthy organisation to deploy it.

Open Consent is being engineered to provide the policy foundation for scalable self regulation, or to paraphrase – Make consent open and transparent enough for people to engage in the control and management of their own personal data control becomes possible.

For example:
A consent record registry can be utilised to facilitate multi-jurisdictional harmonisation of consent requirements for use on the Internet, it can do this with a common receipt record as a baseline, a common process for consent renewal, and redress.

With such a baseline, countries or companies can utilise trust marks as intermediaries to handle different types of privacy related consent and sensitive data sharing issues. Intermediaries can then provide certified auditing, depending on industry, and type of sensitive data.

[30] Ibid. 2

Trust marks can be active consent technology on consent receipts, which give people access to contextual consent tools and redress mechanisms.

As such, rather than forwarding complaints directly to a regulator, the trust services (represented by trust marks) would be an initial point to redirect complaints from people to companies/organisations.

Multiple trust marks, or multi-jurisdictional requirements can then be combined into a consent receipt and made available to the service user in the consent context. Thus providing the scalable infrastructure for cooperatively regulating consent.

The aim with developing Open Consent is to build in the best of breed privacy codes of practices, consent standards and consent notice legal requirements.

Providing an inherent and systematic mechanism to measure and compare the privacy protection proffered by each trusted service/mark/ and or protocol, in terms of policy transparency and consent.

In such a framework open consent enable people who provide consent (and receive consent receipts) to have an active role in overseeing the compliance of their own data use and control, fueling growth in the trust services who audit the practices of organisations in each sector, industry and jurisdiction.

In such an architecture, a privacy seal representing the PIPEDA privacy trust/legal framework would be competitive globally and be a channel for a new level of engagement from the global business community.

What's more, this infrastructure then provides the environment for standardised icons, and terms of use to be developed, not only from companies to users, but for terms from people to services and companies. This is an area where an intense amount of innovation is starting to happen. For example, the Customer Commons led User Submitted Terms[31] (no stalking icon) project in the Kantara Initiative, and the developing standard for creating icons, packed with permissions, from the British Standards Institute starting Sept, 2nd 2016. (BSI, PAS 4891)

[31] Hodder, M,. 2016 "User Submitted Terms" [July 2016] https://kantarainitiative.org/confluence/display/infosharing/User+Submitted+Terms+project+overview

The founding role of Digital Catapult: Personal Data & Trust Network

"The Digital Catapult was established by Innovate UK as a centre to help unlock new value by lowering the barriers for sharing closed or proprietary data" in order to "unlock productivity growth in the UK's data economy..."[32]

The number one mechanism being exploited by Digital Catapult is to 'enable critical infrastructure for the sharing and flow of closed or proprietary data' by supporting the development of platforms, recommendations and other market intervention actions'. A key area where inefficiencies exist is the "lack of control and trust over personal data sharing."

As a result, these objectives identified by Digital Catapult, resulted in the launch of the Personal Data and Trust Network in March 2015. This network was established to accelerate the discussion around personal data and trust themes by bringing together vision from SMEs, Universities, Corporates, regulatory and standardization bodies.

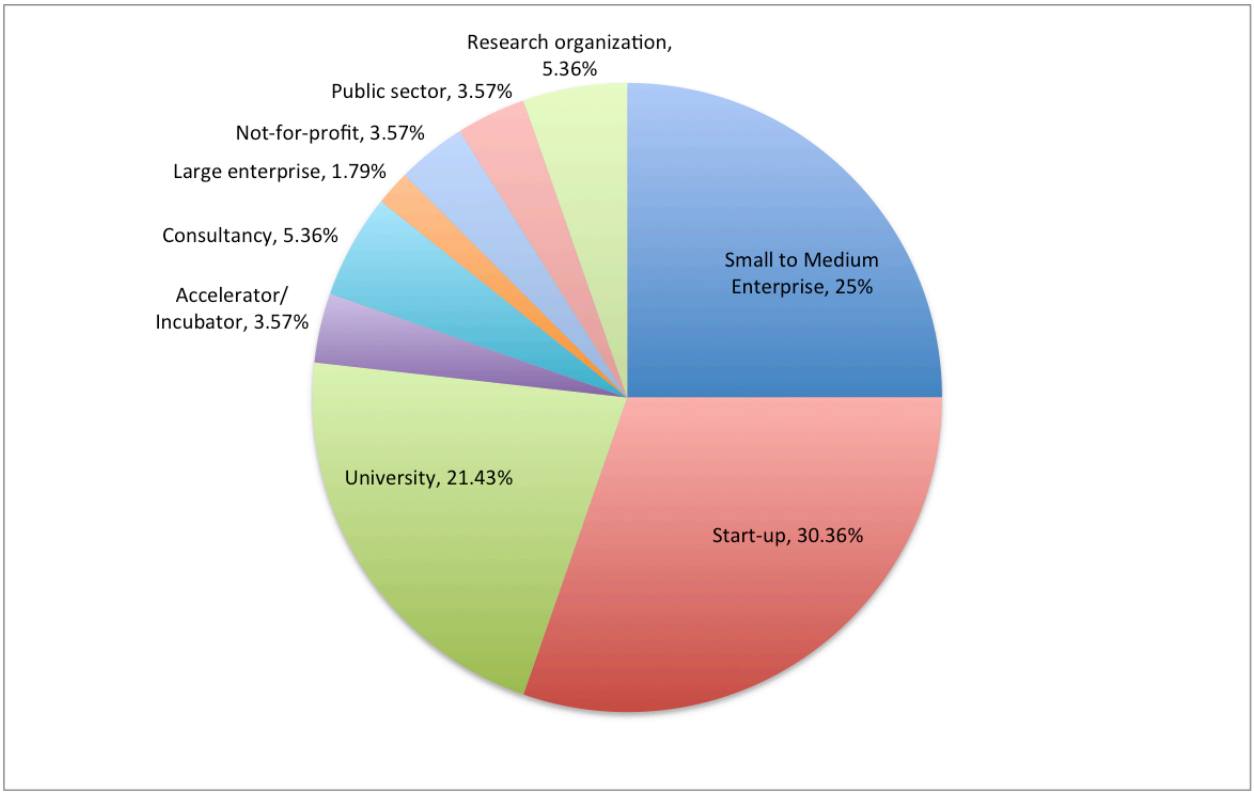
Addressing these challenge areas is often too financially risky and complex for market forces alone, therefore, an effort like the Open Consent Framework requires coordinated mechanisms that bridge the effort of governance internationally, within the private and public sectors, in order to create effective links between the supply and demand side of the market and regulation. Supporting frameworks like the OCF, from Digital Catapults perspective, will enable SME's to translate concepts into commercial products in this space in order to support this ecosystem at scale.

As such, "the Digital Catapult's personal data and trust challenge area works to unlock productivity gains through:

- Unlocking barriers that prevent sharing of personal data to open up opportunities to develop new markets and enterprise.
- Acting as a neutral and trusted partner to convene experts in personal data and privacy to develop an industry roadmap to overcome inefficiencies and barriers in the development of new opportunities"[33]

To accomplish these goals Digital Catapult established the Personal Data & Trust Network, since its inception this network has collected (600) organisations with more than 15% of them focusing on Open Consent.

[32] Parris, S, Spiisak, S, et al, 2015 "The Digital Catapult Productivity: A framework for productivity growth from sharing closed data", http://www.rand.org/pubs/research_reports/RR1284.html [July 2016]
[33] Ibid. 26



Through a series of Real Consent workshops (real-consent.org), sponsored in part by the Kantara Initiative, Digital Catapult has been a key facilitator to operationalizing the OCF, as a trust framework initiative. "Empowering individuals to share their data to address the lack of consumer trust that obstruct the data sharing benefits for individuals and businesses."[34]

Objectives identified by Digital Catapult, resulted in the launch of the Personal Data and Trust Network in March 2015. This network was established to accelerate the discussion around personal data and trust themes by bringing together vision from SMEs, Universities, Corporates, regulatory and standardization bodies.

> "The Digital Catapult was established by Innovate UK as a centre to help unlock new value by lowering the barriers for sharing closed or proprietary data" in order to "unlock productivity growth in the UK's data economy..."[35]

The number one mechanism being exploited by Digital Catapult is to 'enable critical infrastructure for the sharing and flow of closed or proprietary data' by supporting the development of platforms, recommendations and other market intervention actions'. A key area where inefficiencies exist is the "lack of control and trust over personal data sharing."

[34] Ibid. 26
[35] Parris, S, Spiisak, S, et al, 2015 "The Digital Catapult Productivity: A framework for productivity growth from sharing closed data", http://www.rand.org/pubs/research_reports/RR1284.html [July 2016]

From this objective, the challenge to identify and create Real Consent was established.

Addressing a challenge area like Open Consent is often too financially risky and complex for market forces alone. Coordinated mechanisms that bridge efforts around governance internationally, within the private and public sectors are required in order to develop an interoperable notice and consent protocol. Effective links between the supply and demand communities are required for market regulation. Supporting frameworks like that being conceptualised in Digital Catapults, will enable SME's to translate concepts into commercial products in this space in order to support this ecosystem at scale.

As such, "the Digital Catapult's personal data and trust challenge area works to unlock productivity gains through:

- Unlocking barriers that prevent sharing of personal data to open up opportunities to develop new markets and enterprise.
- Acting as a neutral and trusted partner to convene experts in personal data and privacy to develop an industry roadmap to overcome inefficiencies and barriers in the development of new opportunities"[36]

The Leadership of the Kantara Initiative

The 'Consent Receipt' specification from the Kantara Initiative (kantarainitiative.org) is the key initial piece of creating open consent. Kantara's investment in international consent for personal data and trust is the foundation for creating interoperability. Kantara Initiative is comprised of a diverse membership of industry, government, and innovators providing a key space to nurture trust between diverse global market players, such as financial services, retail, healthcare, social enterprise and of course, people.

The Kantara Initiative: Consent & Information Sharing WG (CISWG)

CISWG has developed the proof of consent, 'Consent Receipt' specification: Implementation Draft[37] and example consent record generator[38] to standardize new consent tech around. The core function of proof of consent is to capture the consent event by creating a record of the consent and the consent notice. Essentially the starting point for additional consent tech integration for communities to collaborate and innovate. We are currently looking forward Digital Catapult, My Data, UMA and Kantara Initiative consent receipt implementations.

---

[36] Ibid. 26

[37] Kantara CISWG, 2016 " Consent Receipt Specification v0.8: Implementation draft" [Online] https://kantarainitiative.org/confluence/download/attachments/76447870/KI-CR08-DRAFT-Recommendation.doc?version=1&modificationDate=1470988059000&api=v2

[38] Kantara CISWG,. " Example Consent Receipt Generator and Documentation " [online July 2016] http://api.consentreceipt.org/

UMA: User Managed Access

> "User-Managed Access (UMA, pronounced "OOH-mah" like the given name) is an OAuth-based protocol designed to give a web user a unified control point for authorizing who and what can get access to their online personal data (such as identity attributes), content (such as photos), and services (such as viewing and creating status updates), no matter where all those things live on the web."[39]

UMA is an open standard from the Kantara Initiative, which provides Enterprise with the capacity to permission their users with independent access control to the manage digital resources, of an Enterprise service, independently.

In fact, the consent receipt project was conceptualised as a way to translate consent into UMA permissions (and therefore dynamic consent compliance).

MyData Finland

The MyData Architecture reference model,[40] which is consent centric, is depicting the next stage in an evolution of the existing global consent (box ticking) framework we experience today, championed by the Finnish Ministry of Transport and Communications.

MyData is a Nordic initiative at the infrastructure level in Finland, being developed by leading Finnish universities, personal data engineers and is directly supported by the Ministry of Transport and Communications. The MyData model, at its core, is about data authorization and consent management, utilizing the consent receipt standard candidate to ignite the MyData ecosystem in Finland. The MyData initiative is currently promoting the world's leading conference in MyData on Aug 30- Sept 2nd 2016, in Helsinki[41].

"MyData is a model that equips individuals to control who uses their personal data, to stipulate for what purposes it can be used, and to give informed consent in accordance with personal data protection regulations. It makes data collection and processing more transparent and it helps companies or other organizations implement comprehensive privacy protections."[42]

---

[39] Maler, M "Kantara Initiative: User Managed Access" [Online July 2016] http://kantarainitiative.org/confluence/display/uma/UMA+FAQ?src=contextnavchildmode#UMAFAQ-WhatisUMA?

[40] MyData reference architecture specifications http://hiit.github.io/mydata-stack/

[41] MyData Conference, 2016 "Advancing Human Centric Personal Data" http://mydata2016.org/ [Accssed July 27th, 2016]

[42] MyData Finland, 2014 "A Nordic Model for human-centered personal data management and processing", http://www.lvm.fi/en/-/mydata-a-nordic-model-for-human-centered-personal-data-management-and-processing-860616

"However, the consents often contain similar elements that could be formatted among standard guidelines. When standardized, consent records can be made machine-readable and easy to compare, bundle, visualize, and process automatically."[43]

Coelition

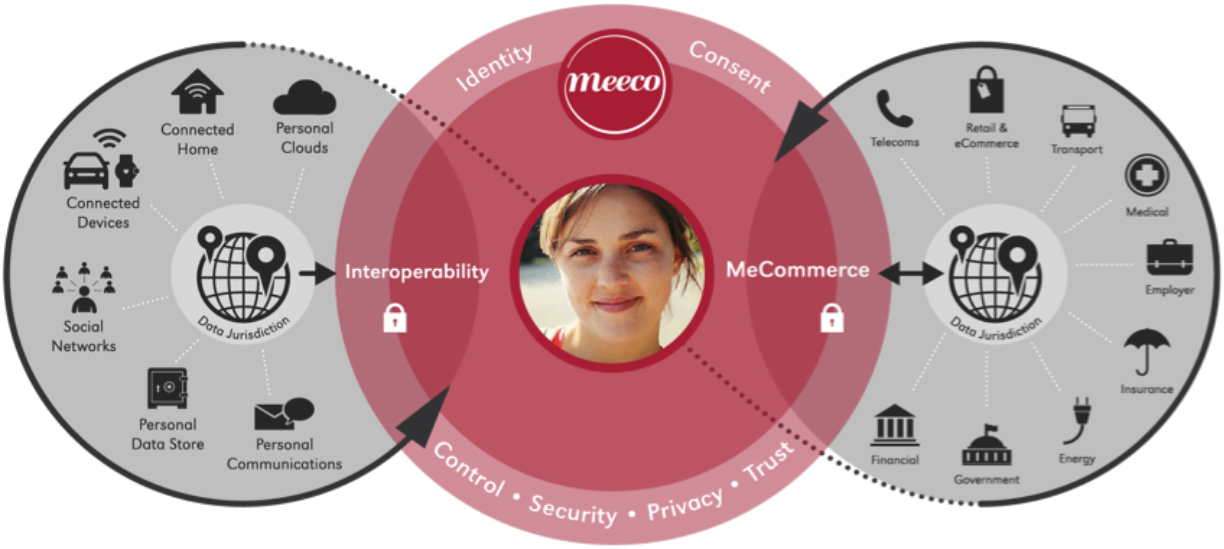
Beyond consent and data ethics, there is the enormous task of making usable the data that enterprise and government hold about people and their behaviour. This includes, big data, IOT data, and very importantly behavioural event data, already generated from the events and activities that are being tracked by organisations and government at scale.

Not addressing these obvious issues in consent is very much a failing of current regulatory systems and consent tech implementations. In many respect, a holistic approach to consent needs to include the limits of consent, and where limits exits, the cross over pseudonymisation and anonymisation trust framework technologies, which are required to be employed in a usable, secure, and trustworthy framework, which the Open Consent Framework is being developed to facilitate.

In this regard, the COEL standard[44] and the Coelition organisation[45] (coelition.org), is an advanced trust framework for behaviour and personal event data. Coelition includes a trustmark that leverages the consent receipt registry, in order to transparently be accountable, and compliant, with EU GDPR. COEL standard and Coelition ecosystem leverages the developing Open Consent Framework and registry by utilising the proof of 'Consent Receipt' specification to record consent events. COEL effectively makes operational the fringe consent topics through consent transparency. Consent receipts enable trust in blackbox algorithms, through trustworthy, standard and transparent architecture. As a result the COEL specification provides a strong basis for interoperability and data portability to large multinational enterprise - enabling the explicit sharing and tracking of behavioural data at scale. Its use in big data and its collection of behavioural data through with IOT sensors and environments represents the next frontier in consent management.

[43] ibid.
[44] ibid.
[45] Langford, Reed 2013 "Data to Life" Coelition (ISBN: 9780957609402)

Meeco



Meeco (www.meeco.me) is a world class life management platform, having been actively in market since 2014. Meeco provides citizens, customers, students, patients and employees the ability to take control and make use of their precious personal information. At Meeco's core is a consent management tool, enabling information to be exchanged explicitly on the terms of the individual, with peers and organisations they trust, through either 'controlled push', or 'informed pull' interactions.

For organisations, Meeco provides an engagement layer to support privacy enhancing customer journeys. Through this model, individuals can use their existing data assets to reduce the time and friction associated with applying for a bank account, updating their insurance or participating in a community research program. Meeco enables 'full-data-give back' as well as explicit, unambiguous consent in each and every interaction.

In this regard, Meeco's core value proposition is enabling people with the controlled push and informed pull, consent-based interactions make possible.

Within the open consent framework context, Meeco will act as the consent receipt repository and interface for citizens, truly providing an interoperable and global platform for the explicit sharing of high value, information rich data. Made operational with the inherent functionality provided to people, enabling them to store, view and manage consent, with the use of consent receipts and the Open Consent Framework.

Conclusion

It is clear, from the above research presented in this response to the OPC, that trust-related risk is significant. For example, "two-thirds of digital identity's total value potential stands to be lost if stakeholders fail to establish trusted flows of personal data."[46] It is therefore essential to not only urge the adoption of the proof of consent specification for interoperability, but also, the co-creation of an Open Consent, which can transcends jurisdictions, utilising the best of breed privacy and legal frameworks, of which PIPEDA is an exemplar.

In this submission we reviewed consent and trust technologies in order to illustrate the breadth of the solutions now available. Focusing on the value and innovation in the UK Digital Catapult, the commitment to infrastructure from Finland's MyData program, the evolving trust technology in the Kantara Initiative community. Introducing Coelition as a trust ecosystem for behavioural, IOT, and big data consent, as well as Meeco as a consumer tool for digital life management, placing the power of personal data control and intelligence in people's hands.

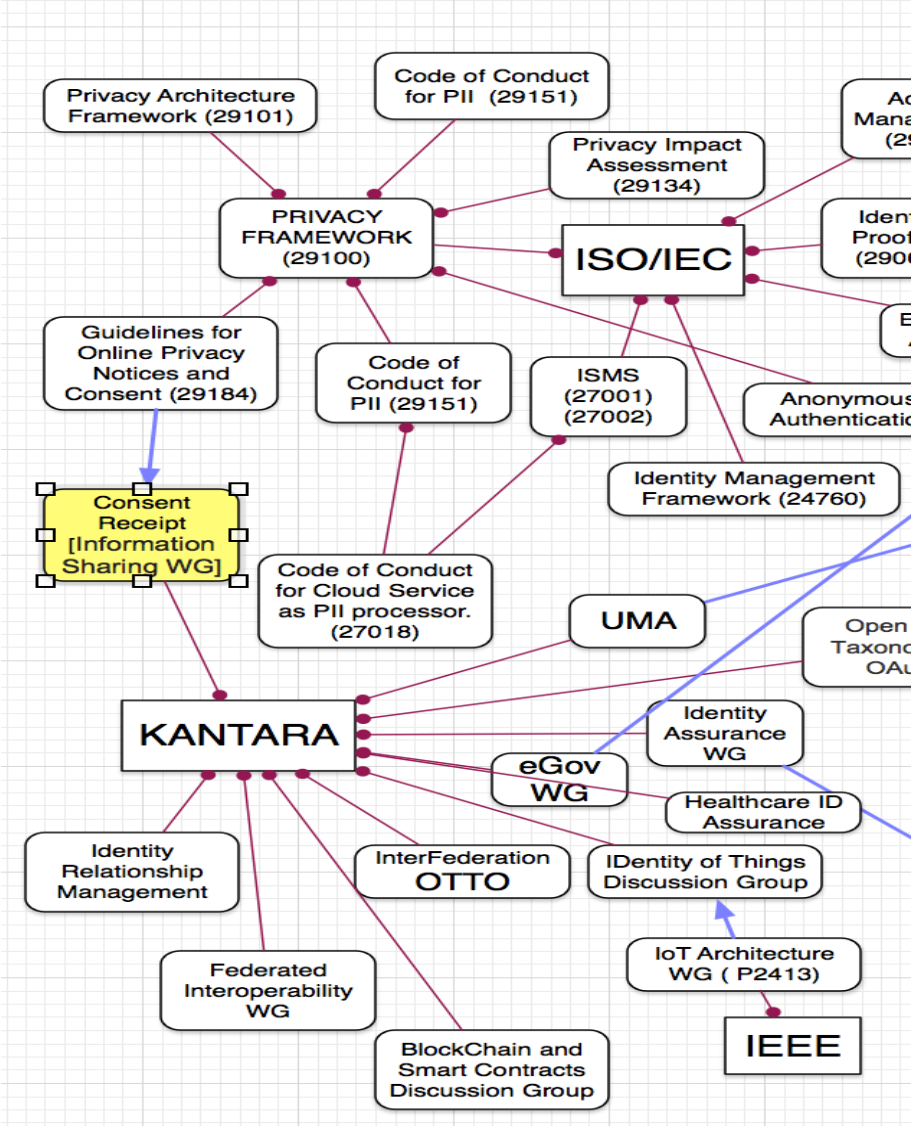
As this effort moves forward in 2016, the opportunity for Canada to harmonise enforcement with international efforts, expand the common standards presented in this paper and lower the barriers for the adoption of the consent transparency is clear. In this regard, we hope to consult and work with the OPC in the future.

[46] Rose,J. Rehse,O. Röber, B, 2012 "The Value of Digital Identity" [July 31] https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/

Appendix A: Standards Gap in OPC Discussion Paper

(Q2) What solutions have we not identified that would be helpful in addressing consent challenges and why?

Question 2, in the call for submissions from the OPC has asked if there are any solutions not identified that would be helpful in addressing consent challenges. In this regard, the maturing standards landscape and the role of standards in the international personal data ecosystem should not only be highlighted, but leverage in any approach to address systemic issues with current consent frameworks. Please find this ecosystem map contributed by Kaliya Hamlin (Identity Woman) which shows the part of the standard ecosystem in which we refer is relevant to consent.


Privacy Architecture Framework (29101)
Code of Conduct for PII (29151)
Privacy Impact Assessment (29134)
PRIVACY FRAMEWORK (29100)
ISO/IEC
Guidelines for Online Privacy Notices and Consent (29184)
Code of Conduct for PII (29151)
ISMS (27001) (27002)
Identity Management Framework (24760)
Consent Receipt [Information Sharing WG]
Code of Conduct for Cloud Service as PII processor. (27018)
UMA
KANTARA
Identity Assurance WG
eGov WG
Healthcare ID Assurance
Identity Relationship Management
InterFederation OTTO
IDentity of Things Discussion Group
IoT Architecture WG (P2413)
IEEE
Federated Interoperability WG
BlockChain and Smart Contracts Discussion Group

Appendix B: Security Trust Assurance Vs. Trustworthiness For People

(Q2) What solutions have we not identified that would be helpful in addressing consent challenges and why?

In the discussion paper, it was clear that there is a blurring of lines between security (assurance to organisations that people are who they say they are) and transparency over the trustworthiness of organisations. The broad use of the term 'trust frameworks' to describe assurance from industry has been effective at confusing what is understood as security and its role in privacy, as oppose to trust worthiness of organisations and their use of consent.

> "[c]ommon deficiencies in our understanding of key concepts such as trust, trustworthiness, cooperation, and assurance in online environments. Empirical evidence from experimental work in computer-mediated environments underscores the promises and perils of overreliance on security and assurance structures as replacements for interpersonal trust. These conceptual distinctions are critical because the future shape of the Internet will depend on whether we build assurance structures to limit and control ambiguity or allow trust to emerge in the presence of risk and uncertainty."[47]

> "These definitions emphasize that calling something "trusted" or "trustworthy" does not make it so. Trust and trustworthiness in computer systems must be backed by concrete evidence that the system meets its requirements, and any literature using these terms needs to be read with this qualification in mind. To determine trustworthiness, we focus on methodologies and metrics that allow us to measure the degree of confidence that we can place in the entity under consideration. A different term captures this notion. Def: Security assurance or assurance is confidence that an entity meets its security requirements based on specific evidence provided by the application of assurance techniques."[48]

[47] Cheshire, C,. 2011 "Online Trust, Trustworthiness, or Assurance?" [July 2016] http://www.mitpressjournals.org/doi/abs/10.1162/DAED_a_00114?journalCode=daed

[48] Clemens University,. "Assurance and Trust" Computer Science 420/620 Class Materials[July] https://www.cs.clemson.edu/course/cpsc420/material/Assurance/Assurance%20and%20Trust.pdf