

RESEARCHING THE TRANSPARENCY OF PERSONAL DATA SHARING: DESIGNING A CONSENT RECEIPT

Author: Tatiana C. Styliari (PhD Candidate at Horizon Digital Economy CDT)
Michele Nati (Lead Technologist Personal Data & Trust at Digital Catapult)

Date: September 2016

CONTENTS

| | |
|--|----|
| 1. Executive summary | 3 |
| 2. Motivation of our work | 3 |
| 3. Researching transparency over personal data sharing: a four-phase process | 5 |
| Phase 1: Internal research | 5 |
| Phase 2: Exploratory interviews | 7 |
| Phase 3: Evaluation interviews | 9 |
| Phase 4: Participatory design workshop | 11 |
| 4. Discussion: is a consent receipt the future of data sharing? | 14 |
| 5. Conclusion | 17 |
| 6. References | 17 |

1. EXECUTIVE SUMMARY

This report presents a three-month research internship focused on the privacy and control of personal data sharing. The aim of the project was to explore how organisations can give more control over the data that individuals share when conducting personal data transactions. We focused on personal data sharing and trust via user experience (UX) design and prototyping methodology. This report describes the process we followed along with findings, and concludes on how the outcomes encouraged us to further develop the tested ideas.

Our main research question was: *How can transparency and users' trust in organisations collecting personal data be improved? Is the idea of a 'consent receipt' a suitable tool for doing this?*

The focus of our study was a thorough evaluation of the UX aspects related to this concept. We started with some internal research mapping of Digital Catapult Centre visitors' journeys in relation to the collection of personal data. The research was carried out through exploratory interviews with Centre visitors, leading to an ideation phase and a first iteration of a 'consent receipt' prototype (a receipt of consent given at time of accessing a service, similar to a receipt for goods purchase)¹.

When the first prototype was ready, more interviews with Digital Catapult visitors were conducted to evaluate the prototype. The Digital Catapult sign-in system was drafted to issue a consent receipt to visitors at the end of the sign in process. The prototype was shown to the visitors who then reviewed it. Based on the collected feedback, a refinement of the consent receipt design followed.

A participatory design workshop concluded our testing of the consent receipt as a way to provide more control, trust and awareness about what personal data people share, with whom, why, when and where. 12 participants, divided into three groups, were given different data-capturing scenarios, underpinning different security concerns and ultimately asked to design their own consent receipts.

The overall participants' response to this project showed positive outcomes for the following reasons:

- 1) The demand for people to know where their data goes is rapidly growing, therefore a consent receipt is seen as a viable solution and provisioning can be easily implemented by organisations
- 2) Organisations could increase their trust and provide better transparency in the data sharing process.

Ultimately, this would lead to the creation of healthier and simpler data privacy policies and would eliminate the problem of agreeing to Terms and Conditions (T&Cs) without being aware of what we are sharing (a recent Eurobarometer survey says 80% of consumers don't fully read the T&Cs)²; as well as losing track and making it difficult to reconstruct of all the data trail we leave behind us, when accessing digital services. This encouraged us to further develop and trial the findings of our study.

2. MOTIVATION OF OUR WORK

To begin with, throughout this report there is a reference to personal data. We follow the EU General Data Protection Regulation's (GDPR) definition of personal data: 'any information relating to an identified or identifiable natural person' [art.2 (a)]. According to a Digital Catapult study³, consumers mistrust how organisations handle their personal data. As a result, business growth slows down, with 65% of surveyed consumers being unsure if data is being shared without their consent.

¹ Consent receipt is a concept championed by Mark Lizar and John Wunderlich from Kantara Initiative and the Consent & Information Sharing Work Group (CISWG) [1, 2].

² http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

³ <https://www.digitalcatapultcentre.org.uk/pdreview/>

The report also shows that there is a need to enhance public awareness and understanding in sharing data as a way to benefit society and deliver economic growth. People usually ignore the T&Cs that they agree to when consenting to give their data in exchange for a service or a product. After a period of time they could have forgotten what they agreed to and as a result can't track who they have given their data to and what happens to it.

As the Internet Technical Advisory Committee has stated: 'It is clear that a common mechanism to encode and publish the policies governing usage of services is needed' [4]. Our aim is to address the '(maybe) read, agree and forget' problem, by evaluating the idea of a 'consent notice' and a 'consent receipt'. The Kantara Initiative Consent & Information Sharing Work Group (CISWG) is currently developing a recommendation for a specification standard for a minimum viable consent receipt.

The consent receipt tries to fill in this gap of notifying people when they share their data. If we were to give a definition we could say that a 'consent receipt' tracks consent by creating a record of it – similar to a regular receipt, which is used to track money [1, 2]. It also allows us to:

1. Understand which data we share, where it goes, who has it and why
2. Keep a proof of consent and enable consistent consent practices
3. Untangle 'obscure' Terms and Conditions documents

Our ultimate project goal is to promote organisations' transparency thus increasing people's awareness, trust and ultimately, control over their data. Our work is focused on helping people to understand why an organisation (in our study, the Digital Catapult) captures their data and what the benefit is. Instead of experimenting with Trust Marks⁴, the effectiveness of which requires time for users to familiarise with it, we aim to achieve this by evaluating the idea of a consent receipt (including visual and textual information). In addition, the consent receipt provides a useful compliance tool, in light of the upcoming enforcement of the GDPR⁵, requiring organisations to show a proof of consent for the personal data they collect from individuals.

We leveraged the consent receipt standard to design and generate awareness of a consumer-centric consent process for increasing consumers' trust in organisations. Therefore, in order to create a meaningful and easy-to-understand consent receipt, we decided to talk with people and understand their real needs and how they would want it to be.

⁴ <https://econsultancy.com/blog/7941-which-e-commerce-trustmarks-are-most-effective/>

⁵ <https://www.privacyandsecuritymatters.com/2015/12/the-general-data-protection-regulation-in-bullet-points/>

3. RESEARCHING TRANSPARENCY OVER PERSONAL DATA SHARING: A FOUR-PHASE PROCESS

The project was divided in four different user-centred phases. Below is a graph that summarises the process we followed throughout the three months.

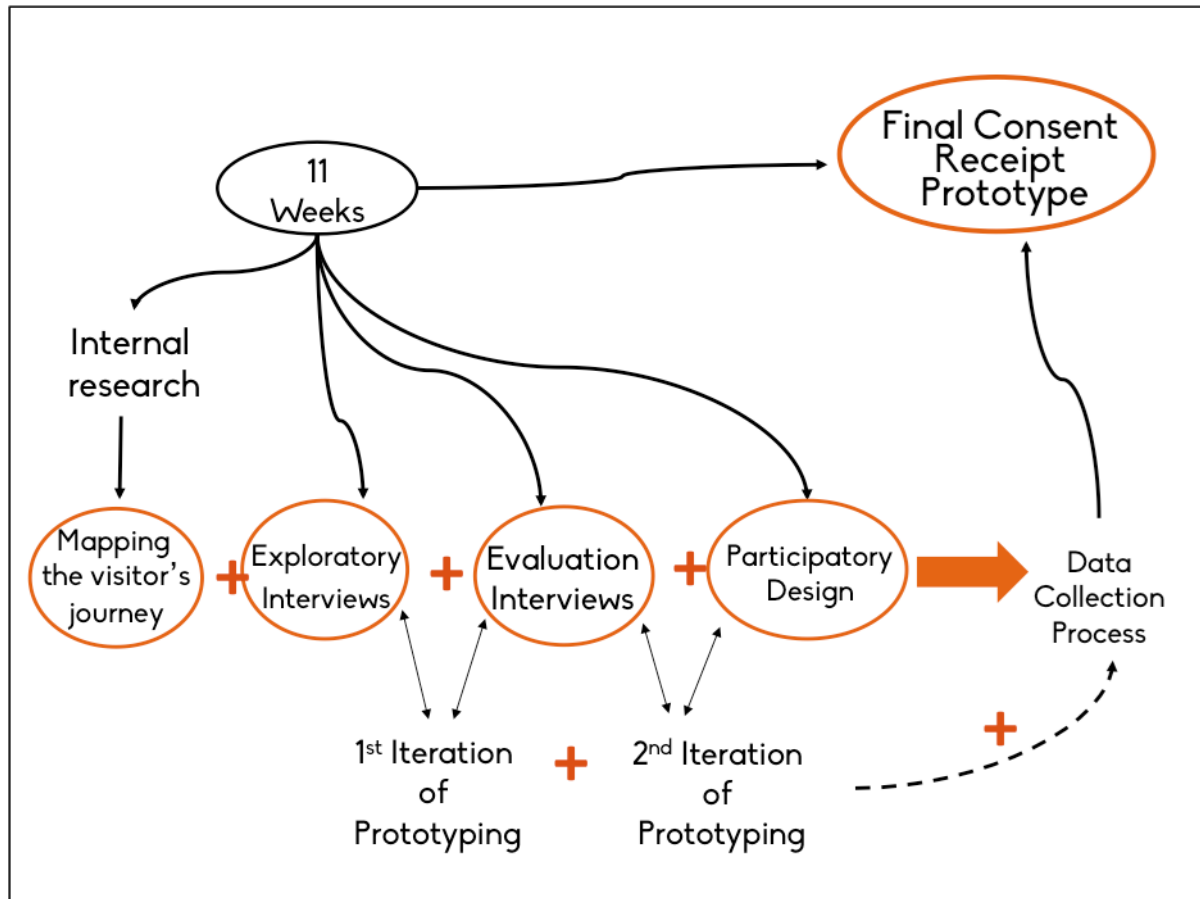


Figure 1: A visualised summary of the methodology followed during the whole project.

PHASE 1: INTERNAL RESEARCH

Initially, in Phase 1 we carried out internal research. More specifically, we talked with employees from different departments of Digital Catapult and observed visitors for a week in order to map their experience. We logged each category of visitor that came to the Digital Catapult, understood what data they shared with us and their experience during their visit. We came up with the maps illustrated below.

The first map (Figure 2) is more generic and provides a summary of all the different visitors' journeys within Digital Catapult, with the main variable being 'the reason for visiting', which then determines the other data collected.

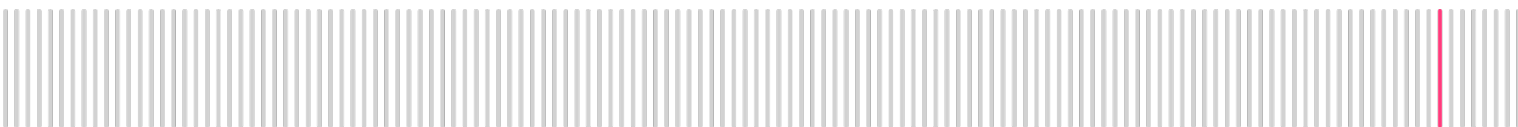
The second map (Figure 3) presents a specific example of a visitor experience – a tour/meeting. It shows the exact journey of a visitor and which kind of data Digital Catapult collects either through its concierge system (Envoy⁶) or through Eventbrite⁷.

| Visit Reason | - | Organisation Type | Means of Data Capturing and Data Captured | Number of Visits | Experience |
|--------------|-------------|---|---|--|-------------------------------|
| Meeting | Employee | Research Organisation - SME - Enterprise - Public Sector - Digital Economy | ENVOY: First time visit/not, full name, email, Institution/company, person to meet, newsletter yes/no (optional), IoTuk (optional). | First time or been here before (data already in) | As described in detailed map. |
| | Contributor | | EVENTBRITE: Prefix, name, surname, email, job title, company/organisation, (not) attended, website, mobile (compulsory), twitter, LinkedIn, newsletter, pass to third party/organisation type> optional and manual upload: they don't get saved. | | |
| Event | Internal | X | Full name, company, attended/not | | |
| | External | | | | |

Figure 2: The general Digital Catapult's visitor experience map.

⁶ <https://envoy.com>

⁷ <https://www.eventbrite.co.uk>



| Related person | Category | Data Captured | Experience | | | Visit Reason |
|---------------------------|--|--|---------------------|---|----------------------|---|
| Operations manager (O.M.) | Visitors tours: academia or foreign dignitaries/ institutes/embassies & consulates, overseas universities. | Envoy registration If big group (20-30) no registration. Personal log with the country, organisation, organiser name, dates, who does the tour. | O.M. welcomes them. | Tour around DC Hear about what DC does Ethos behind the design Why it's situated here It depends on the area of focus of the group. | O.M. shows them out. | Explore the venue/showcase Relationship building Trying to set up similar innovation programme overseas. If trade delegation: expert talk for a couple of hours. |

Figure 3: One example of where internal research led us in terms of understanding the visitor's experience with respect to personal data capturing.

PHASE 2: EXPLORATORY INTERVIEWS

After understanding how data collection is conducted for each kind of visitor and observing what visitors observed about, how they reacted to and interacted with the sign-in experience, we moved on to Phase 2. Due to the bigger control group and therefore amount of data captured that we can utilise through our on-site sign-in system, we decided to focus on this group of visitors.

Phase 2 consisted of 19 exploratory interviews with random visitors of Digital Catapult Centre, aiming to understand what they value in terms of the capture of personal data and how the development of new forms of transparency over personal data sharing, such as the consent receipt, could enhance their experience.

The sample was quite diverse (Figure 4) with respect to age range and professional interest. There is a prevalence of male over female participants, which was representative of the Centre's visitors on the specific day of data collection. As the 'Interest' pie chart shows, a mixture of different people, with different backgrounds and expertise were interviewed (namely not only experts in privacy and personal data protection), which makes our study more neutral and unbiased.

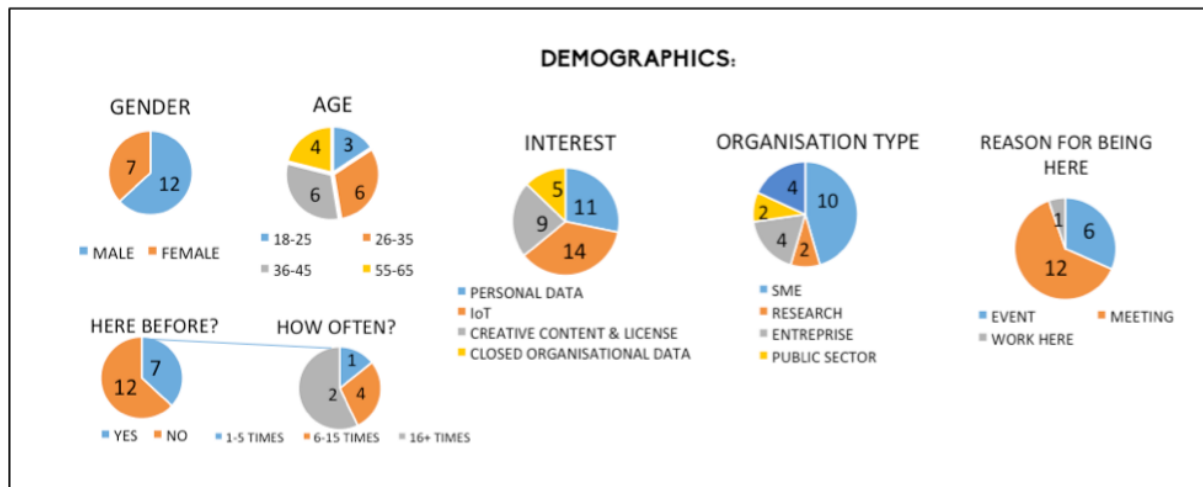


Figure 4: Demographics for the first data collection method. Some values differ from the number of the participants (19) as they had the opportunity to express multiple choices.

The main observations that came out in the analysis are summarised below and can be segmented in two categories:

One was related to the data capturing perception of the visitors, where they had to answer questions such as “Do you trust sharing data with us?” “Why do you think we capture your data?” “Which information and how much is too much in data sharing?”

Understanding data capturing

“You want to build up a profile of the types of visitors, who you are marketing to, research is key to driving any business. I understand the value of research.” (P1)

Sharing data depends on trust in the organisation

“I trust what they are doing with my personal data. Anything I trust in, I would be willing to give all the information asked.” (P3)

Quality & quantity of data shared

“I am giving professional details; I don’t have concerns in terms of the use of data, when it’s my own personal address it’s slightly different.” (P4) “Email, name & organisation: nothing too intimate.” (P2)

The other one was related to the receipt itself where we talked about its necessity, its design, content and implementation. Respondents had to answer a set of questions including “Do you think a consent receipt could be useful?” “Why?” “How would you imagine it?”

Identification/establishment of the problem

“There are some T&Cs that are impossible to read, because if you are just on time for a meeting you don’t have time, and you won’t actually go through it.” (P18)

The end product must be: time efficient, easily accessible, user friendly

“(Make this tool...) very simple and quick, not cumbersome, mobile accessible’ (various participants).”

How did this Phase inform our prototype?

Once feedback was received, we focused on three main areas regarding the design of the consent receipt: Content, format and when it should be given in the process of the visit. In regards to content, we had to make sure that the consent receipt would be user friendly with icons that illustrate:

- **Why we collect this data (use/purpose)**
- **Where and how long we keep it (storage)**
- **Which data we keep on the visitor (content)**
- **Who has it (sharing)**
- **Option to 'forget me' (deletion)**

With regards to the format, it was apparent from the interviewees that static, on-screen consent notification at time of sign-in, and an opt-in/out email as a consent receipt would be the most appropriate. There were three other options: Save as a digital wallet, download as PDF, save in Dropbox.

In regards to when notification should be given to visitors, we determined that if it was shown before they signed in it would be a consent notification, and if they signed in and decided to keep it in their archive as an email, it would be a consent receipt. When coupled with the option to ask for data removal, we agreed that issuing a consent receipt after sign-in was enough to achieve our goal of giving easy-to-understand notice and a record of given consent.

PHASE 3: EVALUATION INTERVIEWS

After creating the first prototype based on what people would value in a consent notice/receipt, we went back to visitors to ask for their feedback. Four influencing factors were ascertained:

1. **Context (venue)**
2. **Scope of the consent (what people consent to)**
3. **Data quantity (how much data they give)**
4. **Data quality (which kind of data they give)**

As value in a consent notice/receipt is dependent on the context that the personal data is collected, we decided to design three groups of questions that we would then randomly ask to visitors. Group A was the control group, Group B investigated the boundaries of visitors in terms of data sharing (which data is 'too much to ask') and Group C set out to identify in what circumstances interviewees would find the idea of a consent receipt more valuable.

There was already quite a lot of trust in Digital Catapult on the part of visitors, as was revealed in Phase 2. Therefore, we wanted to test that if we tweaked the way we did things, how would people perceive the value of a consent receipt? Our main research question was: 'Does the receipt we prototyped increase visitors' understanding of, and increase trust in, how we currently collect data?' We also asked the respondents to answer what they think is needed to make such receipts effective as practice.

There were 26 respondents - nine for group A, nine for group B, and eight for group C. Again, there was an obvious prevalence of male over female participants, which is a representative number of the Centre's visitors on the day of data collection. The age range varied, which gave us diversity within the sample and the chance to see how both younger and older generations think about data sharing and privacy.

The overall sentiment was that only some of the participants were positive about the concept - they liked it, but it wasn't perceived as something that will make huge difference to sharing of personal data in such circumstances.

We suggest that this is due to the fact that Digital Catapult is already trusted as a brand, so there is enough clarity and confidence in the way it operates. Additionally, it also has to do with the fact that the data provided by visitors is minimal and not sensitive – something that was indicated by the participants themselves when they were asked how they would rate the data captured (1 for minimal, 2 for normal, 3 for too much). However, there was a great understanding of the concept and of its necessity, especially in other contexts such as those investigated in group B and C where levels of trust differed (e.g. in the case of data collected online by a recruitment agency).

One of the most interesting conclusions was that in time it is worth getting this practice widely adopted and investigate if and how other organisations and users/citizens will adapt to it. This came out of discussions with some participants on how only one consent receipt is perhaps not useful on its own but alongside many consent receipts, used in every data transaction, they will be powerful and can change the way we trust organisations and share our data.

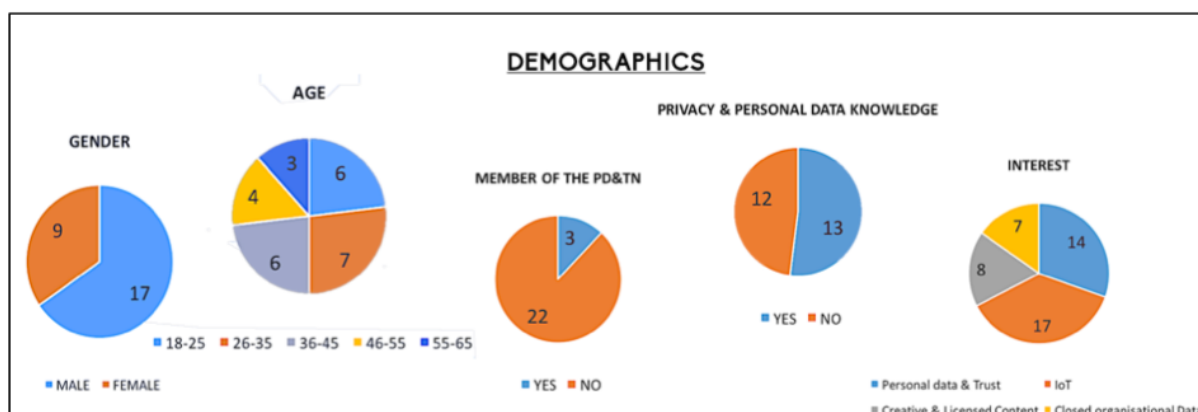


Figure 5: Demographics for the second data collection method. Some values differ from the number of the participants (26) as they had the opportunity to express multiple choices or they didn't want to answer.

The main findings are summarised below:

- Big understanding and acceptance of the concept
- Data breach frequency is very high but people don't know who to address when their data is breached (a consent receipt gives this information)
- Alternative names that emerged from the interviewees:
- User notification | verification receipt | trustee notice | general consent form | proof of data storage | data guarantee/assurance | data consent | consent confirmation | data protection form/user protection form | data usage summary | consent summary

- The interviewees identified many benefits that the consent receipt would have for users, such as:
 - Clear and easy way to understand data policy/T&Cs | reassuring to know what is being done with your data | best practice for visitor | more control over your data | feel more informed | creation of commitment | promise towards each user | more willing to share if I know what it's for
- The alternate settings that were identified by the interviewees and where a consent receipt would be highly valuable were the following:
 - Wi-Fi sign-in | online companies | online purchases | recruiting agencies | home letting agencies | online networks subscriptions | insurance companies | Oyster card top-up | traveling services.
- 14 out of 26 interviewees chose to be sent the consent receipt email so they could keep it as an archive.

How did this Phase inform our prototype?

This phase led us to update our prototype in terms of design, wording and content. We added a timestamp, an email address that users could use to reach the data controller team, changed one of the section's name (from use to purpose) and the way the purpose for data is expressed. Users' feedback also helped us to understand the range of value of the consent receipt, depending on the users' trust in the venue/organisation.

We validated that the prototype should be very short but could include links that would lead to a website with more details for those interested to read more.

PHASE 4: PARTICIPATORY DESIGN WORKSHOP

On Friday 15 July 2016 we conducted the final Phase of the project: a participatory design workshop with 12 participants.

The aim of the workshop was to test the validity of the consent receipt produced already, by getting the perspective of people who would receive it. We wanted to see how they would design it, in order to be easily understood and user friendly. We divided participants into three groups of four and gave them three possible service scenarios to design a consent receipt:

- 1) Your data is very controlled, no sharing (Digital Catapult event/high level of trust)**
- 2) Your data is somehow controlled, shared with some organisations (train ticket online booking service/medium level of trust)**
- 3) Your data is loosely controlled and shared with many third parties (recruitment agency/low level of trust).**

The reason we created three different scenarios was to investigate boundaries and limits in personal data sharing. All groups were asked to prototype consent receipts for all three scenarios. The participants (demographics indicated in Figure 7) were shown a list of ‘ingredients’ that they should consider when thinking about what to include and prioritise in the contents of the consent receipt (Figure 6).



Figure 6: These are the ingredients that should be considered for the consent receipt standard. The above is a combination of the data analysis along with the original standard from Kantara Initiative.

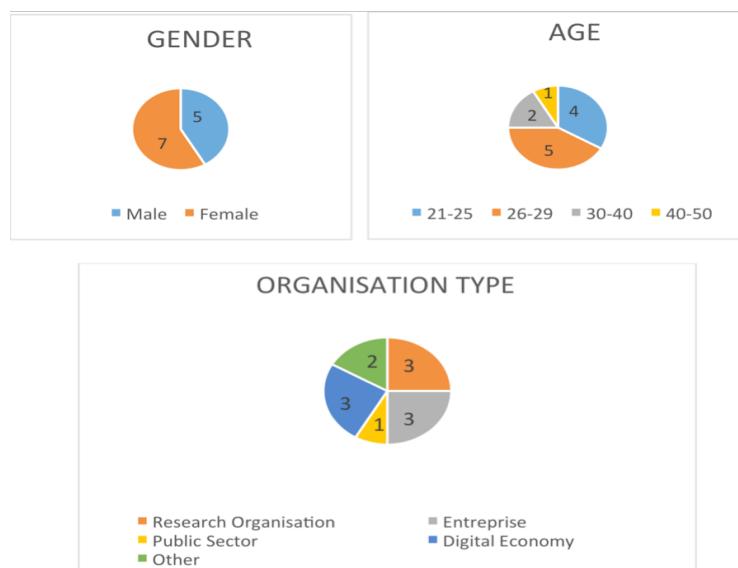


Figure 7: Demographics from the third data collection method.

The main findings of this workshop are summarised below:

Group A

- This team didn't provide a design of the receipt, but rather a summary of the basic concept behind it
- All scenarios share the same basis: they should all have the same information but depending on how higher or lower the level of security is they would have more or less information to protect themselves in case the data is leaked to someone they don't want to have access to it
- Use symbols to show the level of risk for each case: Potentially similar to the traffic light symbols used on packaged food - green, amber and red
- Provide web links to give more information on each specific section. This group wanted to see the contact information clearly and would prefer to contact someone within an organisation directly (by phone) in case something unwanted happened

Group B

- Expected the receipt to be universal
- The 'who' must be stated first (who is collecting the data, the Unique ID and date/time stamp)
- A graphical representation of what exactly is being shared, how it's being shared and who with
- If the data is not shared, an organisation should at least state how it's used and stored so that users know this as a minimum
- To include a disclaimer: How long and where data is being stored and how to change that or opt out
- Include a thank you notice at the end

Group C

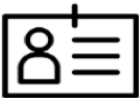



- Basic information has to appear on the top for easy access
- To explain, in a table, that company A gets this amount of data, company B gets this amount of data, so it's easier to track what's shared with whom
- Create an algorithm to limit how long data is being used, shared and kept. For example, if a person is looking for a job, data should only be kept for a specific time, i.e. until they have found employment
- A data specialist/department has to be there to contact in case issues arise
- The purpose for the data capturing needs to be transparent. I.e. even when a person goes to an event, an organisation or third-party can extrapolate what their line of work is, what their income is, their living standards etc

- Output/idea: If a person's data is used by a research organisation they should know what this organisation is doing with it. There needs to be a place/platform that people can access to see what has been produced externally with the use of their data (different from purpose)
- Data storage might be outsourced because it's a big organisation, so users also need information about the outsourced company
- More visible embodiment of the data captured and the purpose for capturing it

4. DISCUSSION: IS A CONSENT RECEIPT THE FUTURE OF DATA SHARING?

This section presents and discusses the final prototype of the consent receipt as formed after all of the data-collection Phases. A mock-up of it is shown below. We reiterate that this project referred to Digital Catapult, however, it explored how the consent receipt would affect consumers in other circumstances and contexts as well. Therefore, the list presented below might be broadened depending on the data collection that each organisation makes.

This is a summary of how your data is used within Digital Catapult:

| | |
|---|---|
| <p>CONTENT</p>  <ul style="list-style-type: none"> • Name • Email • Organisation • Date of visit • Person you visited • Newsletter opt-in/out | <p>STORAGE</p>  <p>Your data:</p> <ul style="list-style-type: none"> • Is stored in a secure location • Can be removed upon request |
| <p>PURPOSE</p>  <ul style="list-style-type: none"> • Health & Safety Issues • Our centre metrics | <p>SHARING</p>  <ul style="list-style-type: none"> • We do not share your data with third parties. |

If you have any questions or doubts about how your information is used by us, please feel free to get in touch with this as receipt at datacontroller@digicatapult.org.uk.

Mon Jul 04 2016 09:26:43 GMT+0100 (BST)
Digital Catapult, 101 Euston Rd, London NW1 2RA, UK

Receipt No:192038

Figure 8: This is the final consent notification as it was structured and refined after all the data collection and prototyping phases.

The **'content'** section refers to the **'what'** (which kind of data an organisation collects). Each individual can have a detailed list of all of the data that an organisation keeps about them and requires their consent. A transparent organisation might eventually also list all of the personal data collected, not necessarily requiring explicit consent (thus making the receipt not only a consent receipt but a 'Personal Data Receipt'⁸).

The **'storage'** section refers to the **'where'** and potentially the **'when'** as well as the **'how long'** the data is stored. If the organisation, for example, deletes the data after one year this should be mentioned as 'kept for

⁸ <https://www.digitalcatapultcentre.org.uk/project/pd-receipt/>

one year'. It would also be helpful to mention when exactly the data is used in case another organisation makes use of it on a specific occasion, e.g. 'use geolocation data only from 8-11am'.

Next, the '**purpose**' section answers the '**why**' an organisation asks for a person's data: What is the main purpose behind their data collection? In our case it could vary between marketing or developmental purposes or simply to capture how visitors are engaging with the organisation and to keep statistics/metrics. Last but not least, there is a section that will be mostly diversified depending on each organisation's data sharing policy with third parties.

The '**sharing**' section refers, therefore, to whether the organisation shares its customers' data with others and if so, who should be stated in a list to provide transparency.

At this point, there needs to be a reminder of a more comprehensive and even more informative version of the consent receipt that would include a clickable button of each section that would link to a webpage with detailed explanation of each section. For example, the 'sharing' section would lead to a list of sharing parties and why a person's data is shared with each one.

At the end of the receipt, we can see the email of the responsible person/team in the organisation, where a user should address any concerns or complaints. There is also a timestamp to indicate when the receipt was issued and a unique ID number so that the organisation can use it to enquire about any issues that arise.

Although a consent receipt could have many advantages for both the user and the organisation, the main benefit is perhaps societal, by triggering a change in the way we conduct data transactions. There are also some limitations and challenges that should be taken into account, which we learned by conducting a preliminary Privacy Impact Assessment for the implementation of a consent receipt into our systems.

First of all, before implementation, there should be set standardised forms of the receipt, which would be followed by all organisations that want to adapt this new tool. Secondly, the organisation that will implement the consent receipt first should be very considerate about privacy policies, take measures against the potential risk of consent receipts' hacking and make sure they have the business processes in place that ensure the deletion of data would actually occur.

Thirdly, there is a chance that some organisations wouldn't want to implement consent receipts because they reveal too much to their customers with one 'quick read', but this is our actual aim: to provide something that would eventually make data sharing fully transparent and that could be moderated and adopted to a wider extent so that all organisations would comply with it. After all, transparency is required by the impending General Data Protection Regulation⁹.

⁹ <http://www.twobirds.com/~media/pdfs/gdpr-pdfs/31--guide-to-the-gdpr--information- notices.pdf?la=en>

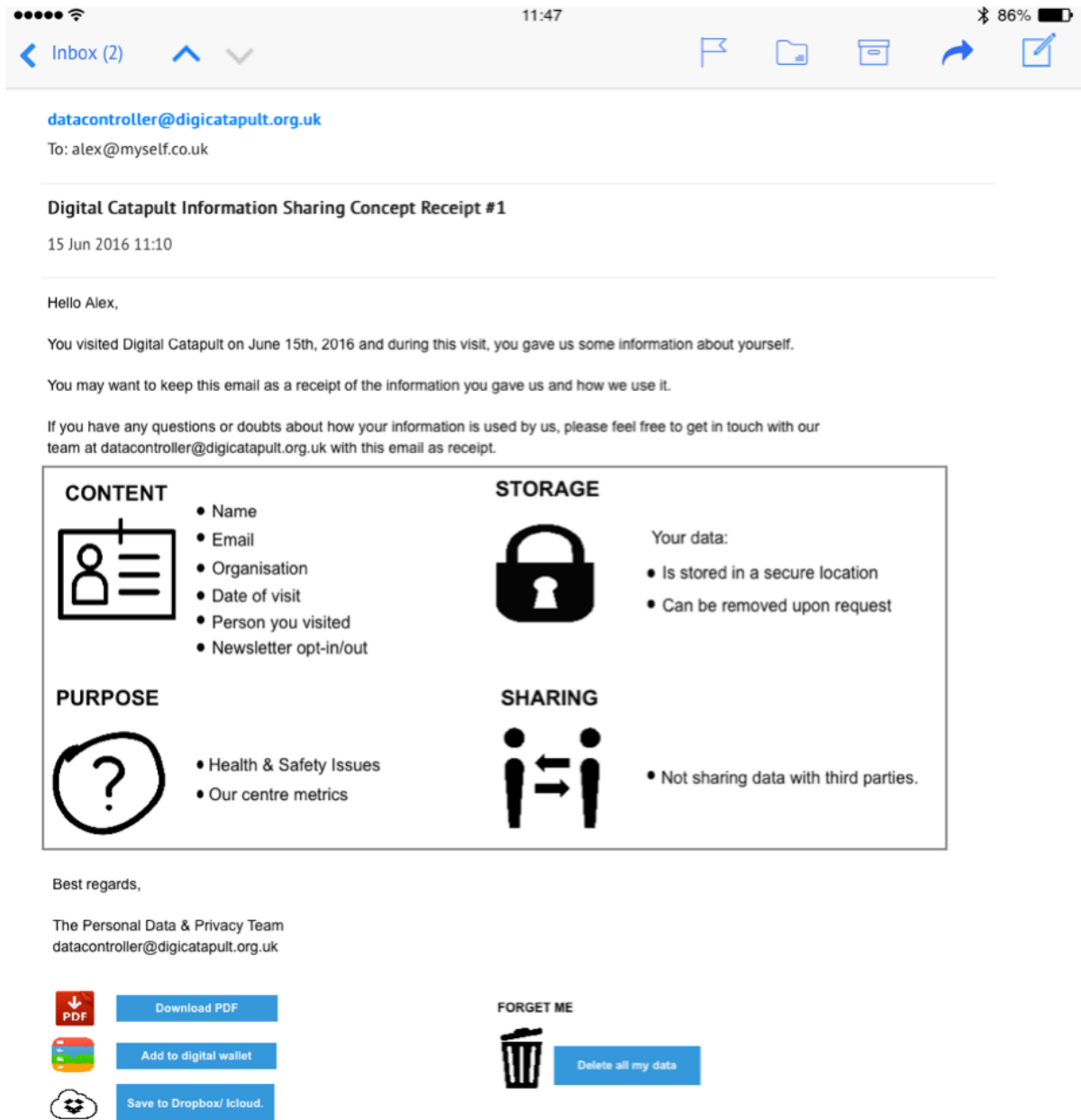


Figure 9: This is the equivalent email that would be sent out to people (after opting in to receive such an email) so that they could have an actual proof of their consent.

5. Conclusion

Following a user-centred approach we explored how people could gain more transparency and be more aware about the personal data they share. To conclude, the project was built on four different Phases: The aim of Phase 1 was to understand our different visitors and how we collect personal data; Phase 2 to focus on the visitors from which we collect personal data from Digital Catapult on-site concierge system (Envoy) and interview them to understand their concern with sharing personal data (if any) and if a receipt (as a concept) increases trust; Phase 3 to evaluate a first real prototype receipt and to understand if it is clear for visitors, if it really increases trust and transparency and finally to gain feedback on the design; and lastly the objective of Phase 4 was for people to design the receipt and see how different it is from what we designed.

As an outcome of this project a new concept has been prototyped using qualitative data collection methods and an iterative process of user experience design. This work contributed to the design of a meaningful consent receipt - in assessing its value in creating transparency and trust in different contexts and in understanding personal data sharing patterns by triggering consent receipts from different organisations, and finally in informing future research.

As a result, the outcome of this project is currently being used and developed further and the concept of the Personal Data Receipt (providing transparency to individuals on all their personal data collected by an organisation) is being trialled with real users at Digital Catapult Centre with the hope that adoption of such transparency practices could be a first foundation of the future of personal data sharing. Evolution of this intervention will require the need for someone to take the lead on building a standard that could be applied to many organisations, educate both institutions and consumers and establish collaborations so that it becomes a prerequisite in personal data transactions. Digital Catapult's aim is to champion such activities.

6. References

- [1] Lizar, M. (2016). Consent Receipt Specification. Available at <https://kantarinitiative.org/confluence/display/infosharing/Consent+Receipt+Specification>
- [2] Brennan, J. and Wunderlich, J. (2016). Consent & Information Sharing Work Group (CISWG). Available at <https://kantarinitiative.org/confluence/display/infosharing/Home>
- [3] Digital Catapult (2016). Trust In Personal Data: A UK Review. Following and Assessing the UK's Journey to Becoming a Data-Driven Nation. Available at: <http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf>
- [4] Internet Technical Advisory Committee (ITAC) (2010). Fostering innovation in privacy protection. ITAC speaking notes for the OECD privacy conference in Israel 25-26 October 2010. Available at <https://www.oecd.org/sti/ieconomy/46952687.pdf>