

# The networked brand identity

Management support tool for tension analysis in brand identity networks concerning privacy

Roelof P. van den Berg

Technische Universiteit Delft





# The networked brand identity

Management support tool for tension analysis in  
brand identity networks concerning privacy

by

**Roelof P. van den Berg**

in partial fulfillment of the requirements for the degree of

**Master of Science**

in Science Education and Communication

at the Delft University of Technology,  
to be defended on Tuesday August 5, 2014 at 2:00 PM.

Supervisor:	Dr. M. C. A. van der Sanden	
Thesis committee:	Prof. dr. C. M. Jonker,	TU Delft
	Drs. C. Wehrmann,	TU Delft
	J.P. Larsen, MSc,	Sense Observation Systems

An electronic version of this thesis is available at <http://repository.tudelft.nl/>.



# Preface

This thesis is the result of my graduation project for the Science Communication track of the masters programme Science Education and Communication at Delft University of Technology. This makes for a double degree in combination with my masters programme for Computer Science at the Interactive Intelligence research group at the same university. The research presented in this thesis was performed as part of an internship at Sense Observation Systems in Rotterdam where I also did my graduation research for computer science.

This thesis is primarily intended for researchers in science communication, brand management, and information privacy research. Reflection on the developed method and its generalisability is given in section 7.2. For those interested in application of the developed method, I suggest reading chapter 3. This thesis is also intended for members of the company, interested in the practical results of the research. The results take form in the practical advice described in chapter 6. A more elaborate outline to this thesis is given in section 1.7.

I would like to express my gratitude to dr. Maarten van der Sanden, my primary supervisor, for his never-ending enthusiasm for my research and our shared passion in decision support for social complexity. Besides my primary supervisor, I would like to thank the rest of the thesis committee and my supervisors: drs. Caroline Wehrmann, Prof. dr. Catholijn Jonker, Janny Ramakers MA, Jan Peter Larssen MSc, for their encouragement, constructive criticism on my research, and for providing a balance between practical applicability and academic value thereof.

My sincere thanks also goes to the people at Sense, Almende, and sibling companies, for their participation in my research, and for the opportunity to get to know the company in which I have explored many of the *identity types* described in this research: through programming a module for Sense's software platform, promoting Sense at a conference, Scoring for the Sense team at the Almende soccer games, meeting clients and partners, giving input on the yearly strategy meeting, and hearing JP's inspiring speeches on jury-sports and other non-work-related topics.

Last but not least, I would like to thank my family, friends, and fellow students for the endless support and numerous discussions. Thank you all for being part of the *actor network* which produced this thesis as an *intermediary* communicating the developed knowledge.

Roelof P. van den Berg  
Delft, July 2014



# Summary

A corporate brand is a complex construct, which might be difficult to manage because of a lack of insight into the network of relevant influencers. Sense Observation Systems (Sense) is a small software company developing software that helps users to get information from the sensor data of their telephones. Sense is aware of the possible threats to privacy users of their products might perceive and wishes to express their vision on privacy in the corporate brand. The communication manager aiding Sense in their external communications works for their parent company Almende. Almende advocates self-organization and the bottom-up approach that goes with it. Sense therefore wishes to manage their corporate brand with as little management as possible. The proposed self-organizing approach is a novelty in corporate brand management.

This research aims to aid the communication manager of Almende in managing Sense's corporate brand. To help the communication manager in this management task, we defined the following research question:

How to manage the corporate brand of Sense Observation Systems so as to encompass the principles on end-user privacy present within the corporation?

## Method

Semi-structured interviews were used to gather insight into how principles on end-user privacy are present within the corporation. A total eight respondents were interviewed: six employees of Sense, and two of the parent company Almende. The respondents cover different functions in the company: four software developers, two managers, and two other members of staff.

A conceptual model for brand management was developed from relevant literature and used to structure the interviews. Six *identity types* were linked to the corporate brand to distinguish between personnel, products, corporate communication, clients, market, and vision. In the interviews was searched for Sense-specific actors (humans, artefacts, policy, organizations, etc.) represented in these identity types. The interviews provided the following information needed for the conceptual model:

- 75 actors from all identity types influencing the corporate brand;
- 7 aspects of privacy relevant for Sense; and
- the distribution of privacy aspects over the actors.

## Results

From the 75 actors we defined 10 representative actor clusters, each cluster consisting of actors with similar associated privacy aspects and from identical *identity types*. For each of the privacy aspects, we visually analysed the tension within the actors network using the *privacy landscapes* defined in the conceptual model. Based upon the preference of Sense employees and network analysis results, we advised Sense to focus on the privacy aspect *use limitation* for which the *privacy landscape* is shown in fig. 1.

We also advised to add more stable elements to the actor network, so that core values become more embedded in the network. The practical suggestions of such stable elements were to develop a corporate slogan, build a product showcasing the corporate values, develop a market strategy leading to clients fitting the corporate values, write out the corporate vision so that it becomes more public.

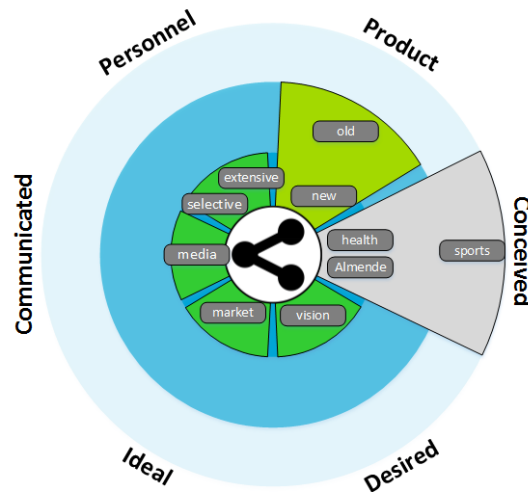


Figure 1: Privacy landscape for use limitation. Use limitation is placed in the centre, with actor clusters confirming the aspect on the ring directly connected. Only the actor clusters *old* and *sports* are not confirming *use limitation*. Attention to these actors can lead to a more stable core concept in the brand identity.

## Conclusion and discussion

The developed *privacy landscapes* enable us to indicate points of attention in the actor network attributing to the corporate brand of Sense. Also, the advice to manage the company brand using stable elements increases the practical applicability; the effort for the communications manager at Almende can therefore decrease over time.

The developed method is a novelty in brand management because of its ability to visually point out actors unaligned to the (preferred) corporate brand. Furthermore, the method provides insight not only in misalignments between but also within *identity types* by the use of actor clusters. Information privacy research might benefit from the observation of the following privacy aspects that were not found in literature: ownership of the data collected about a person, restriction of access to user data for the company where data is stored, how ownership is distributed in issues concerning multiple parties, and the depersonalisation of data so that it can not be traced back to an individual.

We believe that the developed method and resulting *privacy landscapes* can be applied to other companies using different concepts in order to find points of attention within the corporate actor network. We recommend to reduce the possibilities for observer bias in the methodology by replacing the individual semi-structured interviews with group sessions. with Participants in such sessions have limited observer influence and can determine concepts for the brand identity and label and cluster actors. Instead of a research approach, the group sessions would be more similar to creative sessions.



# Samenvatting

Een bedrijfsmerk is een complexe constructie, die moeilijk te beheren kan zijn vanwege een gebrek aan inzicht in het netwerk van relevante beïnvloeders. Sense Observation Systems (Sense) is een klein softwarebedrijf dat software ontwikkelt die gebruikers helpt om informatie te krijgen uit de sensordata van hun telefoons. Sense is zich bewust van de mogelijk door de gebruikers van hun producten ervaren bedreigingen voor de privacy en wil hun visie op privacy uiten in het bedrijfsmerk. De communicatiemanager die Sense helpt in hun externe communicatie werkt voor hun moederbedrijf Almende. Almende pleit zelforganisatie en de bottom-up benadering die ermee gepaard gaat. Sense wil daarom hun bedrijfsmerk beheren met zo min mogelijk actieve sturing. De voorgestelde zelforganiserende aanpak is nieuw in het management van bedrijfsmerksmerken.

Het doel van het onderzoek in dit proefschrift is de communicatie manager van Almende te helpen bij het beheer van Sense's bedrijfsmerk. Om de communicatiemanager in deze taak te helpen, is de volgende onderzoeksvraag gedefinieerd:

Hoe kan Sense Observation Systems het bedrijfsmerk beheren waarin de principes voor eindgebruikersprivacy zijn geïntegreerd?

## Methode

Semi-gestructureerde interviews werden gebruikt om inzicht te verwerven in hoe principes op privacy van de eindgebruiker aanwezig zijn binnen het bedrijf. Er zijn in totaal acht respondenten geïnterviewd: zes medewerkers van Sense, en twee van moedermaatschappij Almende. De respondenten hebben verschillende functies binnen het bedrijf: vier softwareontwikkelaars, twee managers, en twee andere personeelsleden.

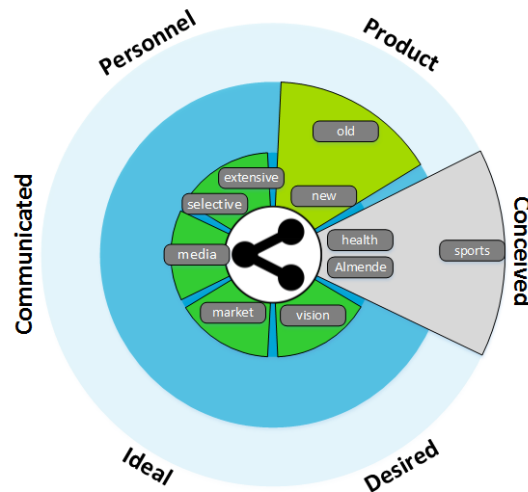
Een conceptueel model voor merkmanagement werd vanuit relevante literatuur ontwikkeld en is gebruikt om de interviews te structureren. Zes *identiteitstypen* gerelateerd aan het bedrijfsmerk werden hierin beschreven welke onderscheid maken tussen personeel, producten, bedrijfscommunicatie, klanten, markt, en visie. In de interviews werd gezocht naar Sense-specifieke actoren (mensen, artefacten, politiek, organisaties, enz.) vertegenwoordigd in deze identiteitstypes. De interviews gaven de volgende informatie die nodig is voor het conceptueel model:

- 75 actoren uit alle identiteitstypen die het bedrijfsmerk beïnvloeden;
- 7 aspecten van privacy relevant voor Sense; en
- de distributie van privacy-aspecten over de actoren.

## Resultaten

Vanuit de 75 actoren werden 10 representatieve clusters gedefinieerd bestaande uit actoren vanuit identieke identiteit en geassocieerd met onderling gelijkwaardige privacy-aspecten. Voor elk van de privacy-aspecten analyseerden wij visueel de spanning binnen het actor netwerk door gebruik te maken van het conceptuele privacylandschap-model. Op basis van de voorkeur van Sense medewerkers en de resultaten van de netwerkanalyse adviseerden wij Sense te concentreren op het privacy aspect *use limitation* (gebruiksbeperking) waarvan het privacy landschap is weergegeven in fig. 1.

We raadden verder aan om stabielere elementen toe te voegen aan het actor netwerk, zodat de kernwaarden meer worden ingebed in het netwerk. De praktische suggesties voor dergelijke stabiele elementen zijn het ontwikkelen van een bedrijfsslogan, het bouwen van een product wat de corporate values demonstreert, het ontwikkelen van een marktstrategie die leidt tot een klantenkring die past bij de bedrijfswaarden, en het schrijven van een bedrijfsvisie waardoor deze duidelijker openbaar is.



Figuur 1: Privacy landschap voor *use limitation*. *Use limitation* wordt geplaatst in het centrum, met de bevestigende actor-clusters op de ring direct verbonden aan het centrum. Alleen de actor-clusters *old* en *sports* bevestigen *use limitation* niet. Aandacht voor deze actoren kan leiden tot een meer stabiel kernconcept binnen de merkidentiteit.

## Conclusie en discussie

De toepassing van de ontwikkelde *privacylandschappen* stelt ons in staat om aandachtspunten aan te geven binnen het actor-netwerk voor het bedrijfsmerk van Sense. Het advies om het bedrijfsmerk te beheren met behulp van stabiele elementen verhoogt de praktische toepasbaarheid; de moeite voor de communicatiemanager bij Almende kan hierdoor in de loop van de tijd verminderen.

De ontwikkelde methode is nieuw binnen merkmanagement vanwege het vermogen de actoren die niet in lijn zijn met de (gewenste) bedrijfsidentiteit te visualiseren. Bovendien geeft de methode door middel van de actor clusters niet alleen inzicht in afstemmingsproblemen tussen de identiteitstypen maar ook binnen deze identiteitstypen. Onderzoek naar informatieprivacy zou kunnen profiteren van de observatie van privacy-aspecten niet gevonden in de literatuur: eigendom van verzamelde data over een persoon, beperking van de toegang tot gebruikersdata voor het bedrijf waar gegevens zijn opgeslagen, hoe de eigendom verdeeld is in kwesties met betrekking op meerdere partijen, en de depersonalisatie van gegevens zodat deze niet herleidbaar zijn naar een persoon.

Wij zijn van mening dat de ontwikkelde methode en de daaruit voortvloeiende *privacylandschappen* kunnen worden toegepast op verschillende bedrijven met verschillende concepten om aandachtspunten binnen het actornetwerk van het bedrijf te vinden. Wij raden aan om de mogelijkheden tot *observer bias* in de methodologie te verminderen door individuele semi-gestructureerde interviews te vervangen door groepssessies. Deelnemers aan dergelijke sessies kunnen met beperkte invloed van de observator, concepten bepalen voor de merkidentiteit en actoren labelen en clusteren. In plaats van een onderzoeksanpak, zijn de groepssessies meer vergelijkbaar met creatieve sessies.

# Contents

<b>Preface</b>	<b>iii</b>
<b>Summary</b>	<b>v</b>
<b>Samenvatting</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Problem description	1
1.2 Research goal	2
1.3 Research question	2
1.4 Research methodology	3
1.5 Scientific and practical relevance	5
1.6 Research focus and limitations	6
1.7 Outline	6
<b>2 Related work</b>	<b>7</b>
2.1 Exploration of literature	7
2.2 Selection of literature	8
2.3 Relevant literature	9
<b>3 Conceptual model</b>	<b>15</b>
3.1 Identity types	15
3.2 Actors	15
3.3 Privacy aspects	16
3.4 Actor clusters	17
3.5 privacy landscapes	17
<b>4 Interviews</b>	<b>21</b>
4.1 Selection of participants	21
4.2 Set-up of the interviews	22
4.3 Expression of privacy	22
4.4 Exploration of identity types	26
4.5 Conclusion	38
<b>5 Network alignment analysis</b>	<b>39</b>
5.1 Network recapitulation	39
5.2 Privacy landscapes	40
5.3 Analysis	40
5.4 Conclusion	42
<b>6 Brand management advice</b>	<b>45</b>
6.1 Privacy aspect selection	45
6.2 Frame of reference	45
6.3 Actions for brand management	46
6.4 Aspects adding to the concept	48
6.5 Other considerations	48
6.6 Conclusion	48
<b>7 Conclusion, discussion, and future work</b>	<b>51</b>
7.1 Conclusion	51
7.2 Discussion	54
7.3 Future work	60
7.4 Bridging fields of study	61

---

<b>A Results per search query</b>	<b>63</b>
<b>B Questionnaire</b>	<b>65</b>
<b>C Interview transcriptions</b>	<b>67</b>
C.1 Developer 1 . . . . .	67
C.2 Developer 2 . . . . .	75
C.3 Developer 3 . . . . .	90
C.4 Developer 4 . . . . .	96
C.5 Staff 1 . . . . .	103
C.6 Staff 2 . . . . .	109
C.7 Staff 3 . . . . .	121
C.8 Staff 4 . . . . .	128
<b>D Labelled actor lists</b>	<b>131</b>
D.1 Developer 1 . . . . .	132
D.2 Developer 2 . . . . .	133
D.3 Developer 3 . . . . .	134
D.4 Developer 4 . . . . .	135
D.5 Staff 1 . . . . .	135
D.6 Staff 2 . . . . .	136
D.7 Staff 3 . . . . .	137
D.8 Staff 4 . . . . .	138
<b>Glossary</b>	<b>139</b>
<b>Bibliography</b>	<b>141</b>

# 1

## Introduction

“Branding is a study in complexity” say Franzen and Moriarty [9], which is often simplified using linear thinking. Often, communication managers miss the insight into the network of influencers to the corporate brand. The corporate brand covers the entire corporation and represents values held within the history of the corporation as well as the values held by employees and founders Kok and Barendrecht [16]. The corporate brand serves to bind all corporate stakeholders to the company and is more complex to manage than a product brand: the daily responsibility is with all employees instead of only the marketing and sales department. The implied complexity for managing communication of a corporate brand is the direct motivation for the research in this thesis.

The thesis deals with the study of the complex construct of the corporate brand in the context of a small software company from Rotterdam, The Netherlands. The problem the company faces with embedding their vision on end-user privacy into the corporate brand is described in section 1.1. Section 1.2 then sets the goal for this thesis regarding the described problem which results in the research question and sub questions defined in section 1.3. We approach the research question using the methodology described in section 1.4. The relevance of this research for both theoretical and practical fields is given in section 1.5, and limitations to the research are explained in section 1.6. The chapter ends with the outline of the report in section 1.7.

### 1.1. Problem description

This thesis deals with the problem of Sense, a software company which is unable to directly reach end-users with its vision on end-user privacy. This section first describes the company, its products, and how privacy concern comes to mind with these products. Secondly, the network surrounding Sense and connecting Sense to their end-users is explored to show the problem of Sense in their effort to reach the end-user.

The company [Sense Observation Systems](#) (Sense) is a young software company. Sense was founded in 2009 as a spin-off by their research-oriented parent company [Almende](#). The company is defined as a small enterprise consisting of 6 regular employees at the time of research. The team of employees mainly consists of software developers involved in developing Sense’s products. Next to the software developers, there is a managing director, and an office manager. Formal communication methods are developed with the aid of the communication manager of Almende.

Software developed by Sense improves context awareness for other applications. For this, they provide the acquisition and storage of data, as well as the intelligence to create meaning out of collected data. An example scenario of this gathering of data is found in this case from health care: Data from mobile phones is used to detect when an elderly person falls on the floor. The nearest available caregiver is then contacted to provide help to the fallen person. Availability of caregivers is determined by monitoring the current activity of each caregiver. The type of software developed at Sense is categorised into ubiquitous computing since its application in mobile phones which are always present near the user for whom context awareness is computed.

Heersmink et al. [12] connects the field of ubiquitous (ever-present) computing to the topic

of privacy. We therefore assume Sense's work in data collection through ubiquitous means is connected to privacy. According to Sense's top management, Sense is aware of the threats to user privacy associated with their field. They aim to make end users aware of the whereabouts of their data, and give end users ownership on their data by letting them decide with whom to share which data. Sense assumes this vision on end-user data privacy is a novelty within their field, also because privacy is not often approached from the end-user perspective. According to Lahlou et al. [18], many software-developers do not take privacy into account due to a variety of reasons: privacy is an abstract problem, privacy is not a problem yet (when it concerns prototypes), privacy is not a problem at all (security and cryptography can solve it), privacy is not their problem (but for society), or it is simply not part of the project deliverables.

Sense creates middle-ware, which implies that a layer of software is developed based on Sense technology. The software built upon Sense technology is the product which reaches end-users. Sense prefers to develop software in co-creation with third parties which serve as problem owner and connection to the end-users. This choice makes that Sense can not directly communicate their intent in relation to privacy to the end-users.

Not being able to directly connect to the (latent) needs of end-users regarding their privacy is a problem for Sense. Based on the observations of Lahlou et al. [18] regarding software-developers and privacy, alignment of visions on privacy may not be present from Sense to the end-user. Respect for the privacy of the end-user can enable companies working with Sense to build a long lasting relationship based on mutual trust and respect with the end-user [19]. The complexity of managing a corporate brand related to a 'soft'-value such as privacy is seen as a problem by Sense.

## 1.2. Research goal

Sense wishes to more directly communicate their vision on privacy to the end-user. Because Sense develops software for, or in cooperation with third parties, their vision is communicated through others. Sense wishes to have these third parties associate Sense with Sense's vision on privacy. Furthermore, Sense wants to see their vision on privacy reflected in the products they create for or with these third parties. The communication manager present at Almende has asked for insight into how this can be achieved through existing communication methods and networks. The goal of this research is therefore to help the communication manager communicate Sense's vision on privacy to third parties with or for whom products are developed.

## 1.3. Research question

The problem description given in section 1.1 states that the communication manager is unable to manage the complex network associated with a corporate brand in a company where the communication functions are distributed amongst all employees. The communication manager therefore wants to know how to manage and communicate the corporate brand related to end-user privacy. The research question based on this problem, is defined as:

How to manage the corporate brand of Sense Observation Systems so as to encompass the principles on end-user privacy present within the corporation?

We define several sub-questions to aid the main research question. In chapter 2, we will first go into the definitions of *privacy* and the *corporate brand*. After these terms have been defined clearly, we wish to know how the corporate brand of Sense is defined and which entities (humans, artefacts, policy, organizations, etc.) have an effect on the brand. Possible entities might be internal and external stakeholders, but also products developed by the company. We define the first sub question as:

**SQ1:** Which entities determine Sense's corporate brand?

After an answer to this question is obtained, it is necessary to know what these entities add to the brand. Regarding the main research question, we focus on how each of these entities values end-user privacy. The second sub question is therefore defined as:

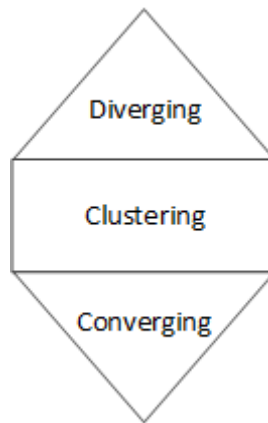


Figure 1.1: The three stage diamond as developed by Tassoul and Buijs [27]

**SQ2:** How are principles on end-user privacy present within those entities?

By finding the values on end-user privacy for each of the entities determining the brand, the remaining question is how to use this knowledge and develop a central element in the brand of Sense. We define this research question as:

**SQ3:** How can principles on end-user privacy become central in Sense’s corporate brand?

The goal of this research is to help the communication manager communicate Sense’s vision on privacy to third parties with or for whom products are developed. Because a well defined corporate brand can add to this goal, and the communication manager needs knowledge on how to manage such an identity, the remaining relevant question for the communication manager is stated as:

**SQ4:** How to manage a corporate brand based upon these principles?

## 1.4. Research methodology

The research in this thesis is set up to provide an answer to a practical question as seen in section 1.3. Before analysis of the practical situation, the relevant theoretical background on the research question is explored. This is then used as basis for interviews wherein the practical situation is researched. Both theory and practice are then combined to analyse the interview results, based upon which practical advice is designed.

The methodology is inspired by methods used in creative problem solving (CPS). As described by Tassoul and Houdijk [28], CPS processes have two basic characteristics: they are comprised of multiple phases, and each of these phases consists of three stages. Each of the phases includes a diverging and converging stage surrounding a clustering stage, creating a three stage diamond [27] as seen in fig. 1.1.

Figure 1.2 shows the complete layout of the research described in this thesis. As can be seen, the methodology uses three diamonds as described above. These three diamonds are used to cover all the research questions posed in section 1.3. The first diamond goes into theory to construct a conceptual model which will enable us to answer the questions posed by the company, as described in section 1.4.1. Using the method described in section 1.4.2, the second diamond explores the reality within the company and matches this to the conceptual model. The second diamond concludes with an overview of the network surrounding the company and thoughts on privacy therein. This insight into the network surrounding Sense is used in the third diamond for the advice described in section 1.4.3, where insights from theory are used to advise the communication manager.

### 1.4.1. Theory

The first phase of research uses theory to build a conceptual model which is used in subsequent phases to solve the main research question posed in section 1.3. In the diverging stage, literature

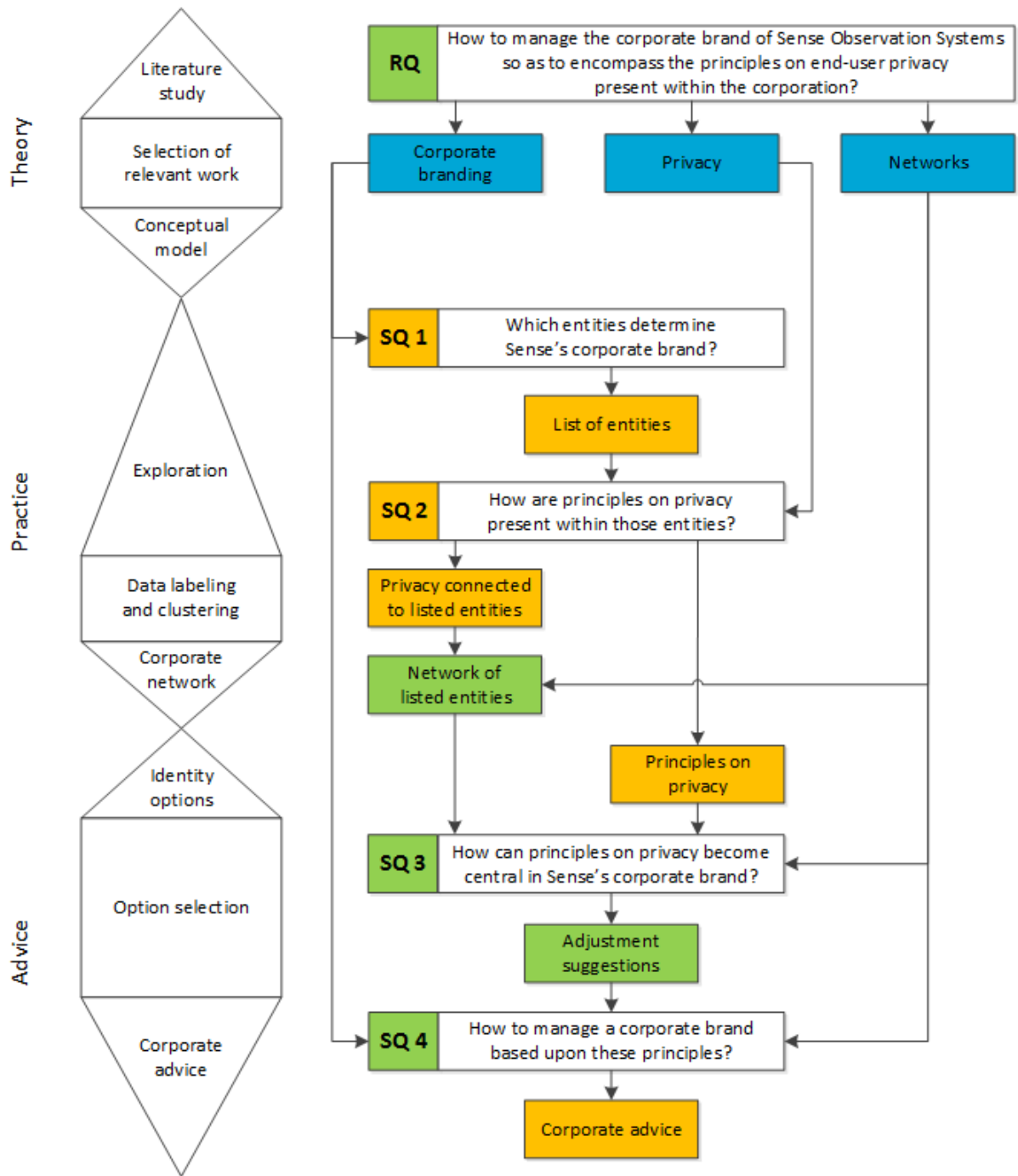


Figure 1.2: The applied methodology of this research linked to three three-stage-diamonds for the phases theory, practice, and advice. Each part of the methodology is categorized as either theory (blue), practice (orange), or both (green)



is sought which is relevant to the research question. The structured method based on the work by van der Sanden and Meijman [30] is used to find relevant literature. Relevance to the research question is found in search queries with keywords related to branding, privacy, networks, and software. More details on the method of searching for, and selection of relevant work is found in chapter 2. The conceptual model built at the end of the first phase is found in chapter 3 and forms the basis for subsequent analysis and advice.

#### 1.4.2. Practice

The second phase of research takes the conceptual model and uses it to describe the actual situation within Sense and its corporate network. We use in-depth semi-structured interviews to obtain detailed descriptions of the distribution of privacy throughout Sense's corporate network. Sense employees are interviewed because of their assumed experience with all parties in the corporate network and their availability to the researcher. A total eight respondents are interviewed: six employees of Sense, and two of the parent company Almende. The respondents cover different functions in the company: four software developers, two managers, and two other members of staff. To preserve diversity in employees' visions on privacy, individual interviews were conducted. Specific details on the interviews can be found in chapter 4. Clustering and labeling of obtained data is performed using the conceptual model, which also contains an operationalisation of the privacy concept. In the converging stage, the clustered data is represented in a network using connections as described during the interviews. The result of this phase is a representation of the company network, the visions on privacy therein, and how elements in the network influence one another.

#### 1.4.3. Advice

The final phase of research takes the network representation from the previous phase as a basis. During the interviews, interviewees were asked which of the principles of privacy they preferred to represent Sense. The options generated from this question are analysed by estimating the points of friction within the network using theory on (network) stability. In the clustering step, those options most central to the company are selected and written down as suggestions for network adjustment. The converging step then combines these options into an advice regarding network stability, and how to improve on it. This practical advice for improvement is given in chapter 6 and is connected to theory through the network adjustments suggestions in chapter 5.

### 1.5. Scientific and practical relevance

The research performed in this thesis fits the definition of design research as defined by [5]. By testing the developed conceptual model through its application to a real world problem, this research addresses a practical problem and provides feedback on the theoretical background on which the solution is based. The networked approach to brand management adds to both theory and practice. Next to this, a solution to the main research question empowers the communication manager.

Decentralized communication is often left outside of theoretical models. Kok and Barendrecht [16], who use the exhaustive model by Balmer and Greyser [2], leave out inter-personal communication, because they find it uncontrollable. Taking inter-personal communication into account as part of the company network and providing insight therein, may prove a valuable addition to existing theories. This insight might provide communication managers with handholds on where to focus their efforts.

The company, Sense, creates products which are greatly adapted to the needs of other organizations before reaching the actual end-user. This may result in loss of clarity of the company's identity and especially vision on privacy. For the company to keep a well-defined identity, this research gives insight in the complexity of the network, and advice on how to use the network to the company's advantage so their vision on privacy can prevail to benefit the end-user.

The combination of theory and practice validates the conceptual model built and theories used, which adds to the theoretical knowledge in the field of corporate communication. Next to that, it also empowers the communication manager of Sense by providing insight in the causal relations within the company network and suggestions for improvement of the corporate brand based upon

theory .

## 1.6. Research focus and limitations

This thesis combines existing theoretical work to create a conceptual model meant to analyse a company's corporate network. The conceptual model is applied to the network of the company Sense to provide this company with insight in managing their corporate brand, as well as validation of the conceptual model itself. Within the application of the conceptual model, only the concept of privacy as part of the corporate brand is used. This is done because of the case specific research question posed in section 1.3.

### 1.6.1. Focus

The company Sense is limited in its product development by the available soft- and hardware created by companies many times larger than Sense itself (e.g. Google, Apple, HTC, Samsung). Influencing these companies with Sense's vision on privacy is not considered in this research. Sense uses co-creation with third parties to create products which will be used by actual end-users. The end-users themselves have no direct contact with Sense, but the third parties do. This thesis will therefore focus mainly on the relationship between Sense and the third parties involved in the creation of software used by end-users for whom privacy may be a concern.

### 1.6.2. Limitations

The research uses individual interviews with all members of the company, making the method applicable for small companies. This is due to the method of data collection, which can be replaced by more quantitative or automated methods to enable application of the conceptual model to larger companies. However, the method as posed in this thesis should not be applied to larger companies.

The observations from many individual interviews make for many views on the company network. Combining these views into one network representation can result in translation errors. In documenting the process thoroughly and showing which views were clustered into the network, reliability of the research is guaranteed.

Participation on the interviews is limited to employees of the company Sense, and its parent company Almende. This is done based upon literature by Gioia et al. [10], which states that employees who have developed a sense of "who we are as an organization" are also able to describe the views on the company of external stakeholders. This limitation to employees of the company limits the corporate network to the external stakeholders directly in contact with the company.

The reader should be aware that the interviews were held within a time-span of one week and provide a snapshot of the network of the company. The conceptual model does not provide registration of change over time, or absolute speed of adoption of concepts within the network. It does give insight in where to apply changes in the network, and which elements will be influenced.

## 1.7. Outline

The steps discussed in section 1.4 are used as chapters in this report. Chapter 2 reviews related work that forms the foundations for the conceptual model used and tested in this thesis. Chapter 3 shows the conceptual model based upon the related work. Chapter 4 shows the results of interviews held as part of the investigation into the company that is Sense. The results of these interviews are analysed in chapter 5. The analysis forms the basis for the strategic corporate communication advice described in chapter 6. The thesis ends with conclusions and recommendations in chapter 7.

# 2

## Related work

This chapter will analyse the problem caught in the research question further via a structured literature review. Using the method developed by van der Sanden and Meijman [30], the most relevant literature available at the time of writing is explored as is described in section 2.1. The evaluation and selection of found literature is discussed in section 2.2. Elaboration on the relevant work used in this thesis can be found in section 2.3.

### 2.1. Exploration of literature

The research question defined in section 1.3 served as a basis for this literature survey. We defined five clusters of keywords to search for relevant literature, related to the research question. The main research question is as follows:

How to manage the corporate brand of Sense Observation Systems  
so as to encompass the principles on end-user privacy  
present within the corporation?

Each of the five search clusters contains one or more terms, connected using a logical OR-operator ( $\cup$ ), which makes that results containing any of the terms are given in that cluster. Some terms contain an asterisk (\*), which makes that any amount of characters may be placed on that location. This enables a search for both "corporate branding" and "corporate brand" by using the search term "corporate brand\*". The quotations used around a search term makes sure that terms consisting of two words only show results where these two words are found in that order, next to each other. The exact representation of search terms used within each cluster is given in table 2.1.

The research revolves around the creation of a brand for the company Sense. The first cluster (B) therefore looks into branding, corporate identity, and corporate communication. Because the research is about suitable principles on end-user privacy, the second cluster (P) focuses on the concept of privacy, and value sensitive design in general. The third cluster (N) helps to look into the network of entities surrounding sense and how this network operates. It therefore uses keywords such as network theory, inter personal, and systems theory. In an earlier version of the main research question, the term trust was seen as relevant because of the apparent mistrust of ubiquitous computing by invasion of personal privacy using these technologies. Because of this, the fourth cluster (T) seeks literature on trust. Privacy was linked to the software developed by Sense because of the categorization in the field of ubiquitous computing by Heersmink et al. [12], and is therefore used as the fifth search cluster (S).

For each of the clusters, two search queries were performed in the Scopus-database: one on Title-Author-Keywords, and one on All available fields. Because of the emphasis on corporate branding, the search query for cluster B was performed on all fields for both search queries. The most relevant results are found where search results for clusters overlap. The overlap between two search clusters is found by placing a logical AND-operator ( $\cap$ ) between the two clusters. Within the Scopus-database, no articles were found when looking for the overlap of all clusters.

cluster	search terms
(B) branding	"Corporate Identity" ∪ "Corporate Brand*" ∪ "Corporate Communic*"
(P) privacy	"Privacy" ∪ "Value Sensitive Design"
(N) network	"System* theory" ∪ "Network theory" ∪ "inter person*!"
(T) trust	trust
(S) software	"ubiquitous comput*"

Table 2.1: The search clusters used for searching relevant articles. Quotes (") are used to find the terms between quotes only in consecutive order. The asterisk sign (\*) is a wildcard indicating that any text may be put on that location. The logical OR-operator (∪) makes that sources using any of the terms bound by it are given as result. The search cluster *Trust* was present in an earlier research question, and therefore part of the literature survey.

We therefore assume that the research question of this thesis has not yet been answered. Articles relevant to the research question were found for queries containing 3 or 4 out of the 5 clusters. The exact amount of results is shown in appendix A.

## 2.2. Selection of literature

Because no direct answer to the main research question is found, we look for literature from which elements can be combined into a conceptual model which helps solve the research question. From the research goal defined in section 1.2, we know that it is in Sense's interest to develop a method which can help the communication manager define Sense's brand identity. Relevant literature therefore contains practical models, definitions, or methods to achieve this goal.

### 2.2.1. Primary sources

From the relevant literature, we use found primary sources to obtain generally applicable theories to combine into the conceptual framework. How each of the primary sources was found is described below:

- The textbook on corporate communication by van Riel and Fombrun [32, p. 70] introduced the AC<sup>2</sup>ID model [3] as a way to integrate diverse approaches to understanding the identity of an organization. Balmer and Greyser [2] were also found as top author in the results of the query for cluster B. We describe the work of [2] and its use for this research in section 2.3.1.
- On privacy, the overview paper by Smith et al. [26] linked to influential (Principles of Fair Information Practice [33]) and validated (Concern For Information Privacy [25]) models used to represent the concept of privacy. We describe both models and their application to this research in section 2.3.2.
- Both Luoma-aho and Paloviita [21] and Hoholm and Strø nen [13] refer to works on actor-network theory (ANT) [4, 20] and even on the work of Michael [22] who applied actor-network theory to the concept of identity. We describe ANT and its use for this research in section 2.3.3.
- The work by van der Vorst [31] was not found through electronic queries. The document was advised by Maarten van der Sanden, lecturer at TU Delft and expert on corporate marketing and communication. Because of its relevance to the search clusters B and N, we assume this source to be relevant. We describe the model on brand stability by van der Vorst [31] in section 2.3.4.

### 2.2.2. Omitted sources

Some of the literature was deemed valuable at face value, but not used. These sources were omitted for several reasons, of which two appeared more often. Some literature was found to be focused on software implementation of privacy measures [17, 23, 29]. This level of detail is not needed in this research where we look for strategic advice on brand management. Other sources applied the terms in cluster N so that they focused on online social networks [11, 15, 24]. We do not wish to limit the explored network to only humans, and therefore reject literature with this focus. Omitted literature is not applied for the conceptual model (chapter 3) and is therefore not discussed in section 2.3.

## 2.3. Relevant literature

This section describes the relevant literature found through the process described in section 2.1. This literature is used for the development of the conceptual model described in chapter 3. Related to the research questions presented in section 1.3, literature on brand management (section 2.3.1), privacy (section 2.3.2), actor network theory (section 2.3.3), and brand stability (section 2.3.4) is presented in this section.

### 2.3.1. Brand management

The AC<sup>2</sup>ID [3] and AC<sup>3</sup>ID [2] tests for brand management were developed by Balmer and Greyser to capture the multiple perspectives on the corporate identity in a single framework. They developed the framework to be pragmatic and it meets the needs of both senior managers and scholars [3]. The core assumption in their work is that the identity of a corporation is not a monolithic phenomenon, but rather distributed in multiple identity types. The AC<sup>2</sup>ID defines five identity types, whereas AC<sup>3</sup>ID adds the brand identity as a separate type under the moniker *covenanted identity*. For readability within this thesis we refer to the *covenanted identity* as *brand identity*. The six identity types present in the AC<sup>3</sup>ID test are the *actual*, *communicated*, *conceived*, *ideal*, and *desired*, and the before mentioned *brand identity*. Balmer and Greyser [3] assume that each of these identity types is connected to each of the others as visualised in fig. 2.1. The identity types are defined as follows [2, 3]:

**Actual identity** is defined by the current attributes of the organization and found in internal stakeholder groups. Both the products offered as well as the values held by employees are embodied in this identity.

**Communicated identity** is best defined as the product of corporate communication, but also derivatives as informal communication are part of this identity. Internal communication stakeholders, marketing partners and the media are involved in shaping this identity.

**Conceived identity** is how the organization is perceived by outside stakeholders. Concepts as image, reputation, and branding shape this identity. Determining which stakeholders are important for the company is part of the management process concerning identity management.

**Ideal identity** is what is considered the best position for the organization within its market in a given time frame. This identity is affected by external events and the choices of competitors. Internal and external stakeholders are involved in this positioning of the organization.

**Desired identity** is found in the hearts and minds of the organization's leaders and is their vision for the organization. Where the ideal identity is often the result of analysis, this identity has more to do with the personality and ego of top management members.

**Brand identity** serves as representative of the covenant between the company and its stakeholders and defines what the organization does and promises its stakeholders.

AC<sup>3</sup>ID enables management to investigate whether the corporate brand is expressed similarly throughout the different identity types. Dissonance caused through a lack of alignment between identity types can potentially weaken an organization and need the attention of management.

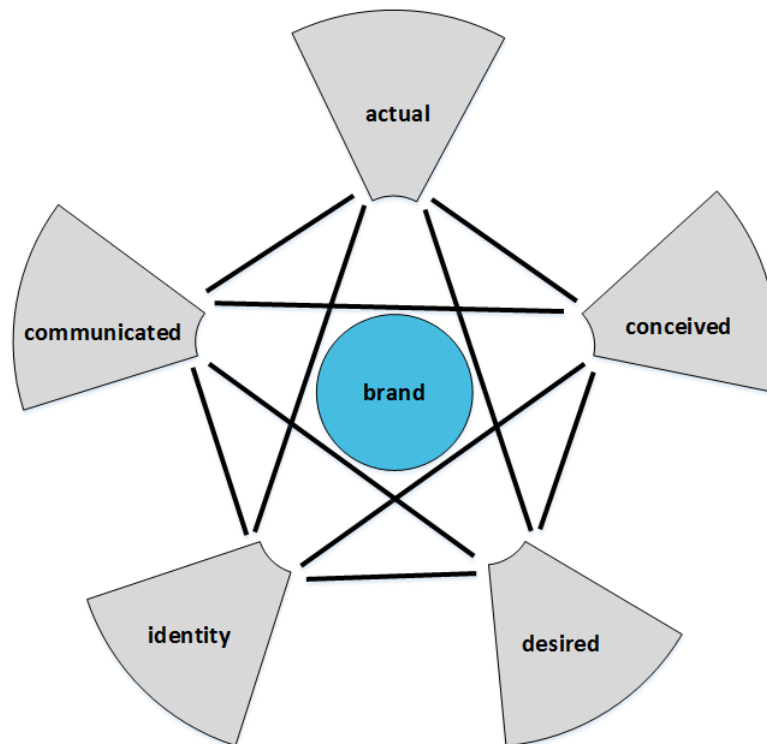


Figure 2.1: The *identity types* in the AC<sup>3</sup>ID-model, with the *brand identity* visualised as a central instead of bounding element.

Not every misalignment of identities weakens the company. Companies can for example choose to create a vision (desired identity) which drives the actual, communicated and thereby also the conceived identity towards a hoped-for future identity by projecting a desired future image. Such desired future images can serve to 'pull' identities into alignment [10] and thereby strengthening them [3].

For the research questions in this thesis, the identity types defined in the AC<sup>3</sup>ID test can serve as a basis with which to find entities relevant to the brand identity. Kok and Barendrecht [16] described the model in detail and applied it to several types of misalignment. They also operationalized the model supplying questions for defining the identities. This operationalization shall serve as the basis for finding entities connected to the brand identity. The AC<sup>3</sup>ID test does not suffice for answering the main research question in this thesis. The method serves to find misalignments between identity types, but lacks the ability to find inconsistencies within one identity type. Because of its general applicability to existing brands, and adjustments to them, the method does not suffice on defining a new core concept for a brand identity. Also, privacy needs to be operationalized to answer the main research question.

### 2.3.2. Privacy

The abstract nature of the term privacy can be seen in its definition such as defined by Wuyts et al. [34] who say that: "obtaining privacy means controlling the consequences of exposing the (possibly indirect) association of individuals to some information/transaction in a given context". Most definitions of privacy are quite abstract and measuring privacy itself is near impossible. Therefore, most of the privacy research relies on the measurement of a privacy-related proxy; an operationalisation of the privacy concept [26]. Lists have been developed which operationalise either the concerns linked to privacy or technical solutions to deal with these concerns. We describe the *concern for information privacy* (CFIP) scale and the *principles of fair information practice* (PFIP), two relevant lists which are also linked together in literature.

Information systems research uses the measurement of privacy concern as the central construct to operationalise privacy [26]. Smith et al. [25] developed the concern for information pri-

vacy scale (CFIP) which was later validated [26]. The scale defines four data-related dimensions to privacy concerns: collection, errors, secondary use, and unauthorized access to information. These dimensions are described as concerns about the following [25]:

**Collection** Extensive amounts of personal information are being collecting and stored in databases.

**Errors** Protection against deliberate and accidental errors in personal data is inadequate.

**Unauthorized secondary use** Information is collected for one purpose but is used for another secondary purpose without authorization from the provider.

**Improper access** Personal information about individuals is readily available to people not properly authorized to the data.

A set of *fair information practices* was used by a US governmental advisory committee to define early privacy legislation [19]. Based on the work of economists Westin [33], seven principles of fair information practice were defined as summarized by Langheinrich [19]:

**Openness and transparency** There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.

**Individual participation** The subject of a record should be able to see and correct the record.

**Collection limitation** Data collection should be proportional and not excessive compared to the purpose of the collection.

**Data quality** Data should be relevant to the purposes for which they are collected and should be kept up to date.

**Use limitation** Data should only be used for their specific purpose by authorized personnel.

**Reasonable security** Adequate security safeguards should be put in place, according to the sensitivity of the data collected.

**Accountability** Record keepers must be accountable for compliance with the other principles.

Although embedded in the legislation of many countries [19], implementation of the seven principles is not often done and designers often lack concern for privacy; privacy is often seen as an abstract problem, not a problem yet, not a problem at all, not their problem, and is often not part of the project's deliverables [18]. In many companies, even though there might be an explicit company privacy policy, the policy is not implemented on a design level. Based upon this apparent lack of privacy policy implementation, we expect a difference between employees' opinion on privacy and the actual implementation thereof in developed software. Because employees and products are both present in the *Actual identity* of the AC<sup>3</sup>ID model [2], we will split this identity type into two distinct types: *Employee* and *Product*. This enables us to better view whether or not this difference is present for Sense.

For the research questions in this thesis, both CFIP and PFIP can serve to operationalize the construct of information privacy. PFIP can be linked to CFIP using the recommended actions for overcoming concerns for information privacy given by Smith et al. [25, p. 192]. Because humans may express their concerns to privacy and Sense's products can only be related to their implementation of the principles of fair information practice, this combination of PFIP and CFIP enables us to interpret and compare responses in the semi-structured interviews for both humans and products. The lack of a (validated) list of indicators for PFIP makes that the principles need further definition through observations in the interviews, which is done in section 4.3.

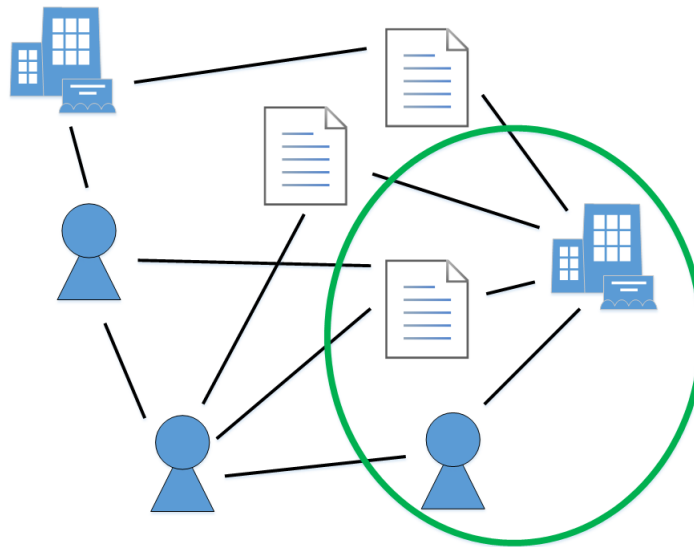


Figure 2.2: Example of an actor-network. People, organizations, and artefacts can be placed into one network. The items in the green circle can be *punctualised* if they represent a stable cluster

### 2.3.3. Actor Network Theory

Actor Network Theory (ANT) is a method used to thoroughly explore the relational ties within a network. Central to ANT is the belief that objects, and not only humans can act to influence one another [22]. For the analysis of material-semiotic networks (with relations between both things and concepts), ANT is an approach where the dynamics between different actors are made visible. Actors are capable of interacting with one another and therewith influence each other. This interaction takes place via so called *intermediaries* which can be scientific articles, computer software, technical artefacts, instruments, contracts, money, but also human beings and the skills and knowledge they incorporate. An actor can be seen as an intermediary that puts other intermediaries into circulation [4].

When clusters of actors within a network reach agreement, they can be reduced to one point in the network from which they originate [4]. This so called *punctualisation* can be applied indefinitely. The example in fig. 2.2 shows a cluster of actors in agreement which can be *punctualised*. In ANT, *punctualisation* is used to be able to move from the micro-social to the macro-social. When a node within the network seems to be the focal point of a controversy between identities, nodes can be expanded into a network as in a reversed punctualisation. By these processes, the dynamics of the network can be explored and abstraction or detail can be added wherever necessary.

ANT has its roots in science and technology studies and should be seen as a method rather than a theory, because it does not usually answer why or how a network is formed [20, pp. 141–156], but rather explores the connections within a network. Michael [22] has applied ANT to the analysis of identity and states that some intermediaries (such as documents, software, and other durable materials) provide stability and make it harder to change the identity of a network as a whole because of their relative longevity compared to ideas in the human mind.

For application to the research in this thesis, creating an actor-network with both humans and objects enables us to put the organizations, people, products, media, and laws present in the identity types of Balmer and Greyser [2]. The act of *punctualisation* described by Callon [4] makes that answers from multiple respondents can be clustered together to form a network representation which is insightful for management.

The nature of ANT is rather abstract for the practical research question in this thesis. However, the act of *punctualisation* and view that actors of different kinds can co-exist within one representation of the world does add to the model of Balmer and Greyser [2] which does not explain the levels of abstraction to take in analysis of the different *identity types*.



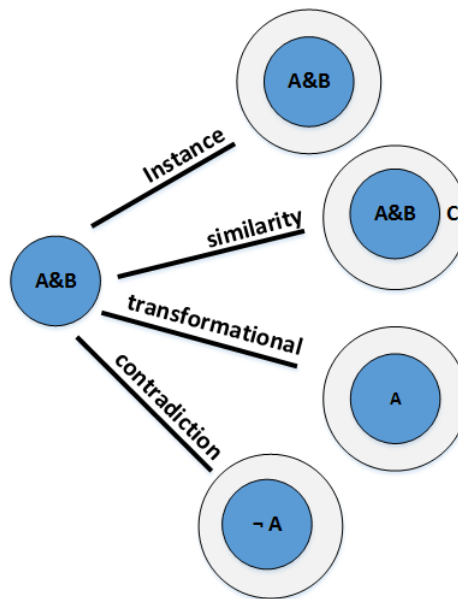


Figure 2.3: Example of the link types defined by van der Vorst [31]. A, B, and C represent core concepts. The blue circle on the left indicates the corporate brand with concept A and B at its core. The four items to the right represent articles showing the different configurations of core concepts which yields different link types.

#### 2.3.4. Brand stability

The work of van der Vorst [31] uses a systems theoretical approach to branding and uses this for brand management. Relevant in his work is the link between the corporate brand and the product portfolio of a company. Both the corporate brand and each of the separate product brands represent a set of values which might differ between products and the corporate brand. By assessing the relations between core concepts and concepts found within the products, the strength of the relation between the corporate brand and each product is defined. four different link types between products and the corporate brand are used by van der Vorst to show these differences. The link types are show in fig. 2.3 and defined as follows [31, pp. 169–175]:

**Instance** All the core values of the corporate brand are present as distinctive subconcepts of the article.

**Similarity** Same as with the instance link, but the article also has distinctive subconcepts of its own.

**Transformational** At least one of the core concepts of the corporate brand does not appear as a central distinctive subconcept.

**Contradiction** At least one of the core concepts of the corporate brand and the distinctive subconcepts of the product brand contradict.

To advise on a corporate brand which best fits the product portfolio and vice versa, three levels of abstraction are used by van der Vorst on which a company can define its corporate brand. Brands which seem to contradict one another on a concrete level might go together on a more abstract level. The following levels of abstraction are defined by van der Vorst [31, pp. 175–182]:

**Taxonomic** The concepts at the level of brand identity define a higher order category of which the article concepts are each a subcategory.  
(e.g. chocolate for the brand, chocolate bar for a product category)

**Feature** The features in the brand identity are found in all articles.  
(e.g. 'safety' for the Volvo car brand)

**Metaphorical** Symbolic features define this frame of reference. The meaning of the concepts is found outside of the product domain.  
(e.g. 'love and security' for the Zwitsal brand)

Three large companies (Mars, Douwe Egberts coffee, and Camel Trophy) were examined by [van der Vorst](#) using his developed methodology. The levels of abstraction were used to suggest changes to the brand concepts on a strategic level so as to improve on the stability of the corporate brand.

For the research in this thesis, the method developed by [van der Vorst \[31\]](#) can serve to define the stability of a brand identity which adopts a certain privacy aspect. We believe that because of the material-semiotic network defined through ANT, we might extend this methodology to actors other than only the products which are used in the work of [van der Vorst](#). We are aware that by using the methodology for a comparison between the brand identity and all actors in the actor-network, we go beyond the application of the methodology to the products developed by Sense. The work of [van der Vorst](#) furthermore gives handholds for a corporate strategic advice which enables us to answer the main research question in regard to brand management.

# 3

## Conceptual model

This conceptual model combines insights from literature so as to help provide an answer to the main research question of this thesis, which is:

How to manage the corporate brand of Sense Observation Systems  
so as to encompass the principles on end-user privacy  
present within the corporation?

Based upon the literature described in section 2.3, the conceptual model builds a visual representation of the actor network influencing Sense's brand identity. Section 3.1 first describes the *identity types* which influence the brand. Section 3.2 describes how discovered actors are linked to these identity types. Section 3.3 continues with an operationalisation of the privacy concept which helps to label the found actors. Section 3.4 describes how to cluster the responses obtained through interviews in order to keep the network manageable. Section 3.5 concludes this chapter with a description of the final visualisation, which is dubbed *privacy landscape*.

### 3.1. Identity types

For determining the best suited brand identity, we will first explore the identity types defined by Balmer and Greyser [3] in the AC<sup>3</sup>ID-model of brand management. This model is augmented with the knowledge obtained from literature on implementation of privacy within software projects, resulting in the actual identity being split up into two distinct *identity types*: *personnel*, and *products*. Because of the use of the models on brand management by van der Vorst [31] and for clarity purposes, we use the term *brand identity* for what Balmer and Greyser [3] call the *covenanted identity*. This results in the set of *identity types* shown in fig. 3.1, which acts as basis for the conceptual model. The positions of *identity types* are kept similar to those used in the AC<sup>3</sup>ID-model by Balmer and Greyser [3].

### 3.2. Actors

Measuring the perception of privacy is done through actors responsible for each of the *identity types*. We consider persons, products, and organizations, as in the definition of actors used in Actor-Network Theory [4]. We use the descriptions of actors found in the work of Kok and Barendrecht [16] to operationalise the identity types defined by Balmer and Greyser [2]. The *actual identity* defined by Balmer and Greyser [2] is split up into the *personnel* and *product* identity to accommodate for a clear inspection of the apparent difference between privacy policy and implementation thereof [18]. A general indication of entities found for each identity type is as follows:

**Personnel** employees, management

**Product** products, services

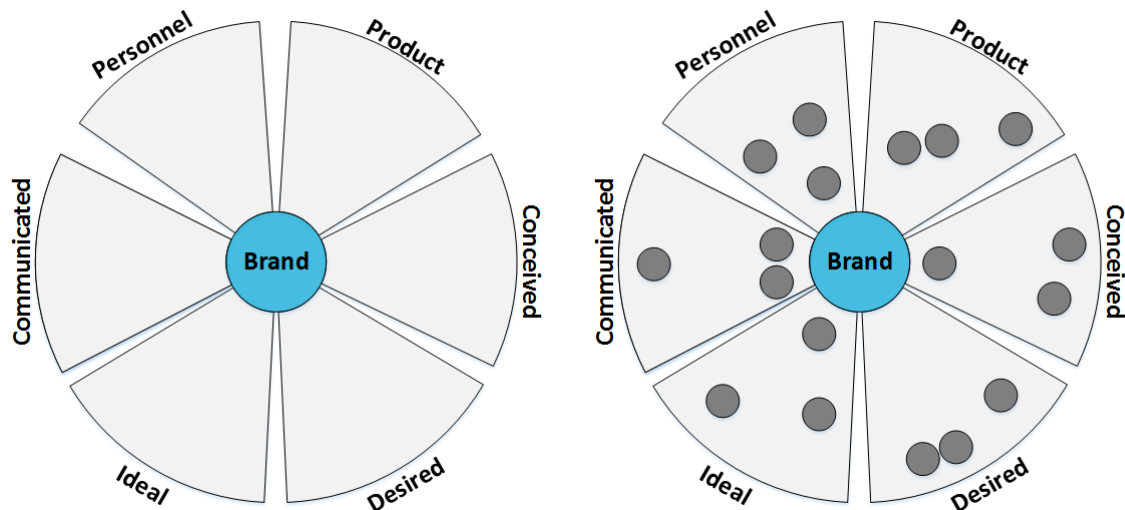


Figure 3.1: The different *identity types* (light grey sectors) linked to the centrally placed *brand identity* (blue circle). Figure 3.2: Each *actor* (dark grey circle) is linked to one of the *identity types*.

**Communicated** corporate communication, media and press, (external) events

**Conceived** partners, clients, prospective clients

**Ideal** competitors, policy makers, legislators, strategy

**Desired** (top) management, vision

These actors are all linked to specific *identity types*, and can therefore be visualized as in fig. 3.2.

The *brand identity* is not defined by actors directly, but rather through the preferred *brand identity* expressed by the respondents to the interviews. As Kok and Barendrecht [16] define the *brand identity* as a “promise that the company has to live up to every day regarding privacy”, respondents are asked what they would want to promise the world regarding privacy if they were the company. This preferred *brand identity* will be used to compare to the results of the analysis of other *identity types* so as to indicate willingness towards a certain aspect of privacy.

### 3.3. Privacy aspects

Privacy values for each of the actors are categorized based upon a list of privacy aspects. This list consists of the *Principles of Fair Information Practice* (PFIP), based upon the work of Westin [19], which covers the design aspects of privacy. Because privacy is a cause for concern [12], we also relate these principles to the concerns found in the *Concern For Information Privacy*-scale [25] (CFIP). PFIP and CFIP are linked together using recommended actions given by Smith et al. [25, p. 192] as well as the description for each of the privacy concerns. This results in the following pairings:

**Improper access - reasonable security** Recommended action against improper access is to implement technological controls on access to systems [25, p. 192].

**Collection - collection limitation** Recommended action for collection is to practice parsimonious database design [25, p. 192], collection limitation is defined as no excessive collection should be made [19, p. 3].

**Collection - openness and transparency** We link “this area of concern reflects the perception” [25, p. 171] to the statement by Westin [33] that “there should be no secret record keeping” [19, p. 3].

**Errors - individual participation** Recommended action against errors is to ensure that applications contain appropriate edit techniques [25, p. 192], where individual participation is defined as the ability to see and correct a record (by the subject of such a record)[19, p. 3].

**Errors - data quality** Static data can become erroneous due to a dynamic world which changes over time [25, p. 173] (e.g. a change of home address), Westin [33] states that data quality involves keeping data up to date[19, p. 3].

**Unauthorized secondary use - use limitation** Recommended action against unauthorized secondary use is to refuse to release personal data to outside entities without explicit senior management approval[25, p. 192], where use limitation defines that "data should only be used for their specific purpose by authorized personnel"[19, p. 3].

No pairing was found for the concept of accountability. Based upon these pairings and the definition of the paired concepts, an association of concepts to the defined privacy aspects is given in table 3.1. Linking these two lists enables comparison of human responses such as concern for privacy (CFIP) and more technical implementation requirements (PFIP). Throughout this thesis, the terminology from PFIP is used. Section 4.3 shows which privacy aspects are encountered during the interviews, and also expands upon the set of privacy aspects based upon those interviews. Applying the found privacy values to each of the actors results in an overview such as seen in fig. 3.3.

Privacy aspect	terms linked to aspect
openness and transparency	informing, secret records, perception
individual participation	access by subject, editing, deletion
collection limitation	purpose for collection, excessive collection
data quality	relevant, up-to-date, errors over time
use limitation	use, authorized personnel, data release, purpose for use
reasonable security	security measures, encryption, sensitive data, protection
accountability	compliance, record keeper

Table 3.1: terms linked to each of the defined privacy aspects so as to enable labelling

### 3.4. Actor clusters

Within one *identity type*, *actors* that value similar *privacy aspects* are clustered into groups. This has the advantage of having multiple observations confirm the *privacy aspects*, and also last longer: a single *actor* may be a one time client, but may come from a sector where more clients come from. This step of clustering is similar to the action of *punctualization* in ANT [4], where groups of *actors* are reduced to a single representation when there is no conflict between them. In this thesis, clustering may also be performed on groups of similar *actors* based upon their sector (e.g. multiple organizations within healthcare). Using this second method of clustering, a general representation can be created using scarce information on the individual actors in a cluster. A visual representation of clustering is shown in fig. 3.4. The *punctualized actor clusters* make for a manageable overview on the different *identity types* and how they relate to the privacy aspects.

### 3.5. privacy landscapes

Stability or fitness of a *privacy aspect* is analysed visually by placing the *actor clusters* in a *privacy landscape* as shown in fig. 3.5. We developed this visualisation to enable analysis of the collected qualitative data in one image.

The *privacy landscape* places the *actor clusters* within the sextant of the *identity type* from which they originate. One *privacy landscape* shows only one *privacy aspect*, and visualises the link of each *actor cluster* to that *aspect*. Each actor has one of the following links to the concept central to the landscape: confirmation, unknown, or contradiction. These link types are inspired by the link types defined by van der Vorst [31, pp. 193–198]. Because the privacy landscape explores only one privacy aspect as possible aspect for the brand identity, the similarity and transformational link

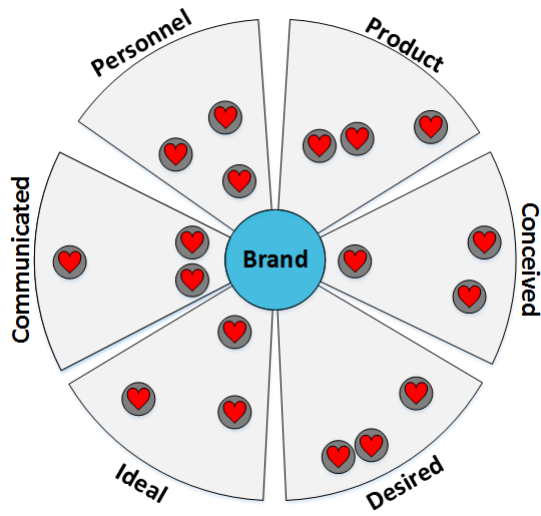


Figure 3.3: Privacy aspects (red hearts) are linked to individual actors (dark grey circles).

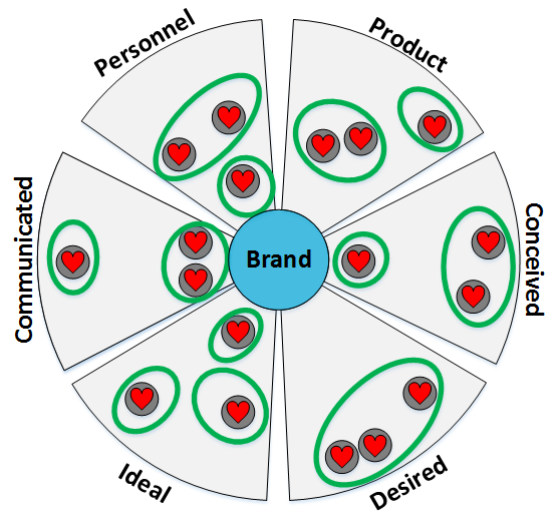


Figure 3.4: Actors within an identity type are clustered when they value similar privacy aspects.

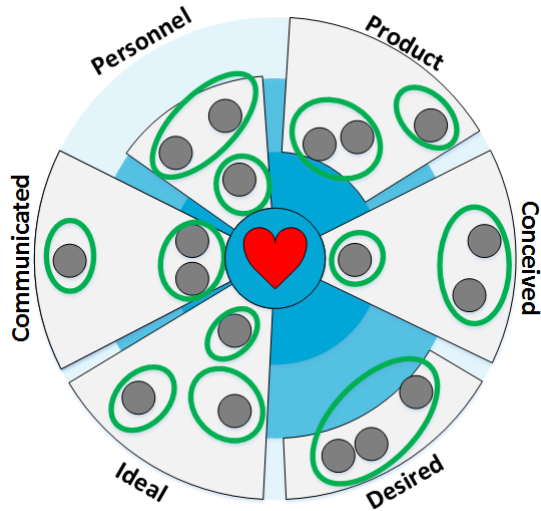


Figure 3.5: The surface of each identity type is shrunk around the actor clusters present on it.

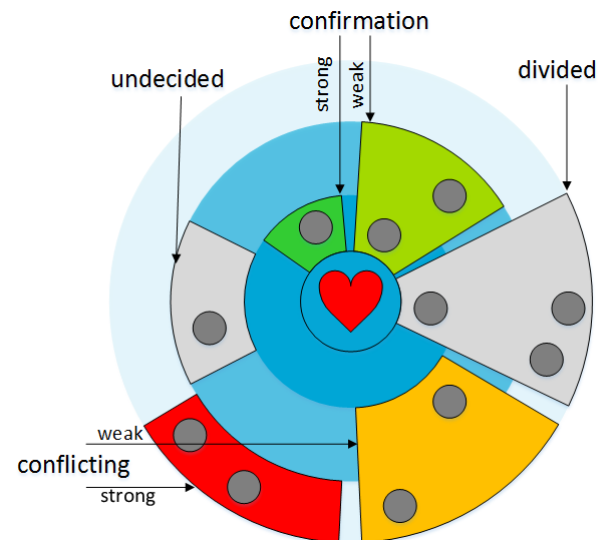


Figure 3.6: Privacy landscape showing different configurations of identity type surfaces: confirming (green), conflicting (red), undecided (left), and divided (right).

by [van der Vorst](#) can not be used. We instead use the *unknown* category to represent clusters for which no attitude towards the central aspect is found through the interviews. The confirmation link is similar to the original and implies that the central aspect is confirmed by the linked cluster. The contradiction link implies that the central aspect is contradicted by the linked cluster. *Actor clusters* with a confirmation link are placed on a ring closest to the central *privacy aspect*, contradicting *clusters* on a ring furthest from the centre, and unknown *clusters* are placed in between. After placement of the actor clusters on the ring indicating their link to the central aspect, each *identity type's* surface shape is reduced in size as long as it still spans the entire set of clusters within it. This method results in six possible configurations of the *identity* surfaces, as can be seen in [fig. 3.6](#). The top two configurations (green) show a positive (confirmation) link to the central concept, whereas the bottom two configurations (red) show a negative (conflicting) link to the central concept. The remaining two configurations are either *undecided* (left) when no clear expression on the value is found in the *identity type*, or *divided* (right) when both *confirming* and *conflicting* values are found.





# 4

## Interviews

This chapter provides the context for the network defined in the conceptual model in chapter 3. Context specific information on privacy beliefs is found through semi-structured interviews. Section 4.1 discusses the choice of participants, and section 4.2 gives the set-up of the interviews. After explaining how principles of privacy were voiced in section 4.3, their distribution throughout different types of identity is explained in section 4.4. Conclusions based upon the interview are given in section 4.5.

### 4.1. Selection of participants

Sense's employees are chosen as participants for the interviews because of their direct involvement in the company and their interaction with the outside world. Based on the work of Gioia et al. [10], we assume that interviewing only internal sources, such as employees and top management, will yield a decent overview of the identity types in the conceptual model.

For investigation into the identity-network described in section 3.1, each of the identity-types in the network is explored so as to fit the corporate situation. Employees can describe the conceived identity, because they have developed some sense of "who we are as an organization" and have communicated and received feedback on the company's identity [10]. We furthermore assume employees can describe the:

**personnel identity** because they are personnel of Sense

**product identity** because of their involvement in development of the products

**communicated identity** because of their involvement in or knowledge of promotional activities

**ideal identity** because of their knowledge of the corporate strategy

**desired identity** because of their knowledge of the corporate vision

The organization chart in fig. 4.1 shows the interview respondents for this research. Six out of the seven employees on the Sense payroll were included in the interviews which were held in July 2012. One employee and all the interns working at Sense were not included because they have not yet developed some sense of "who we are as an organization". Two employees of the parent company Almende are interviewed because of their roles in external communication, and the vision of Sense. Of Sense four employees are software developers, and two have a managerial or staff function. For privacy purposes, the names of participants are made anonymous. Therefore, the participants are known as DEV1, DEV2, DEV3, and DEV4 for developers and as STAFF1, STAFF2, STAFF3, and STAFF4 for staff and management. The difference between developers and different staff functions is made to put responses into perspective.

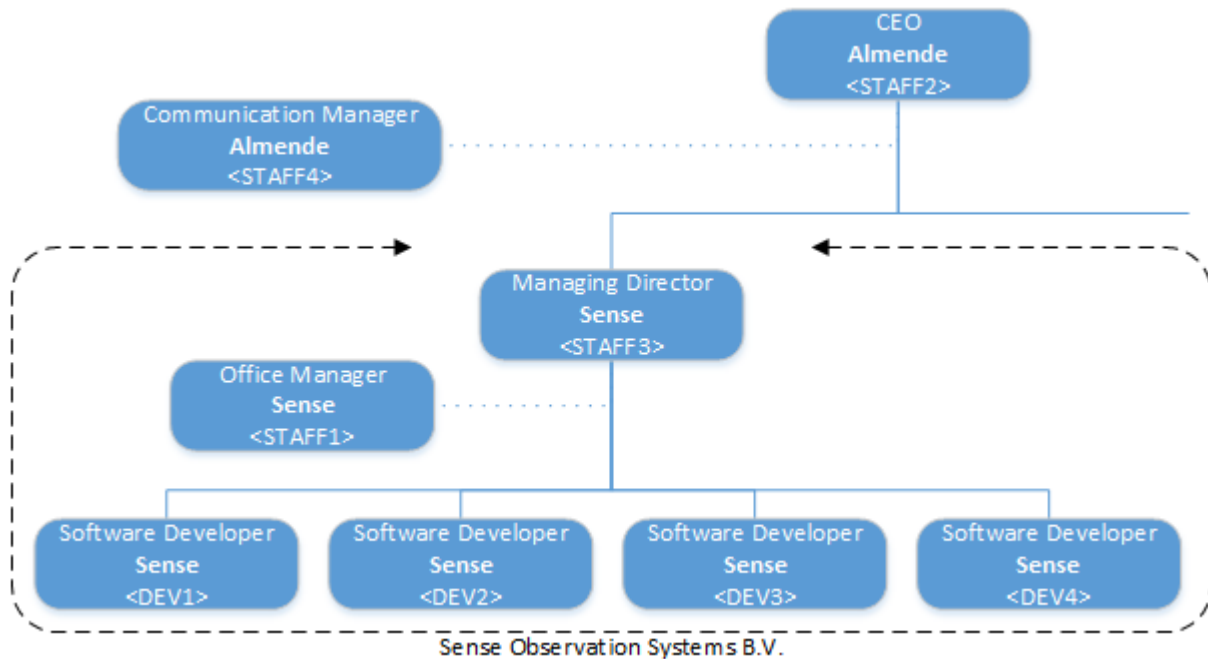


Figure 4.1: Organizational chart showing the interview respondents and their position in Sense or Almende.

## 4.2. Set-up of the interviews

The interviews are semi-structured and consist of three parts. The list of interview questions is found in appendix B.

In the first part, respondents are asked about the actors (humans, artefacts, policy, organizations, etc.) related to each of the identity types defined in the conceptual model. Identity types are hereby explored in a specific order: personnel, products, communicated, conceived, ideal, and desired. This order puts identity types closer to the respondent first, those with which the respondent has less contact come last.

The second part of the interviews discusses the visions on privacy for the actors explored in part one. The respondent is asked for his personal definition on (end-user) privacy and how the actors from part one adhere to this definition. Differences between those actors are found in this part.

The last part of the interview explores the brand identity. The respondent is asked what he wants to promise the world if he would be the personification of Sense. The interview is rounded up by asking what is needed in the network to make their preferred brand reality.

In the following sections, quotes from the interview-transcripts are used to clarify observations. The transcripts themselves are found in appendix C, and the labelled set of actors described by each participant in appendix D.

## 4.3. Expression of privacy

This section gives insight into how types of privacy were expressed during the interviews. The previously defined aspects of privacy are provided with examples in sections 4.3.1 to 4.3.7. Next to the privacy aspects defined in section 3.3, some of the answers given in interviews require the definition of new privacy aspects. These types are given in section 4.3.8 and section 4.3.9, after which conclusions as to which privacy aspects are used in the results of the interviews are given in section 4.3.10.

### 4.3.1. Openness and transparency

This cluster is associated with informing individuals about records kept about them or keeping such records secret. From the interviews, we conclude that the terms “transparency”, “insight

into use” and “(clear) communication” are being associated with openness and transparency.

An example of transparency in the definition of privacy is given by DEV4, who states the following as part of his definition of privacy regarding the use of Sense products:

“Dat je transparant bent en mensen duidelijk maakt wat de gevolgen zijn.” (page 99) translates into: “That you are transparent and make the consequences clear to people.”

STAFF3 names “insight into use” in his definition of privacy, which connects to transparency:

“Inzicht in wie dat gebruikt voor welke doeleinden.” (page 124) translates into: “Insight into who uses it and for which purposes.”

An example of communication is given during first communication with potential clients, where concern about secret record keeping is voiced as told by DEV4:

“Het is wel vaak zo dat mensen vaak beginnen met ‘O, Big Brother!’” (page 101) translates into: “It is often the case that people start with ‘Oh, Big Brother!’”

Communication on privacy can originate at different points, as is clear from this comment by DEV3:

“We hebben het er zelf meestal niet over, meestal andere mensen.” (page 94) translates into: “We usually do not talk about it, mostly other people.”

#### 4.3.2. Individual participation

The cluster of Individual Participation is associated with the ability of a user to see and change their personal data. From the interviews, we conclude that both “changing”, and “deleting of personal data” is associated with this cluster. Especially staff members voiced their opinion on the ability to see and change personal data. STAFF2 said:

“De data is van jou dan mag je het dus ook veranderen, je mag het deleten, je mag er vanalles mee doen wat je wilt.” (page 121) translates into: “The data is yours, so you may change it, you may delete it, you may do all sorts off things as you like.”

Where the definition of Individual Participation within PFIP (section 2.3.2) uses it to make sure that data is kept up-to-date, the management of Sense see the data as a means of communicating ones personal state. And whether or not the communicated state equals what actually happened is up to the user. As STAFF3 puts it:

“Als er wat anders naar de wereld gecommuniceerd moet worden dan wat er is waargenomen, dan moet je dat natuurlijk zelf weten.” (page 124) translates into: “If something else needs to be communicated as was observed, that is up to you.”

#### 4.3.3. Collection limitation

The principle of Collection Limitation is associated with preventing the excessive collection of information. Due to the nature of Sense’s products, it is difficult to apply this principle on Sense’s business. The applications of Sense collect sensor data from e.g. mobile phones and derive state information from it. Because of the artificial intelligence used, it is often not known whether or not specific sensors are relevant for specific states. STAFF3 states that it is not up to Sense’s employees to decide if too much data is being stored:

“Ik kan niet beslissen of iets te veel of te weinig data is.” (page 124) translates into: “I can not decide if something is too much or too little data.”

#### 4.3.4. Data quality

Data quality is defined in the PFIP as the practice of keeping data relevant over time. Within the Sense software, sensor data is stored so as to train user state recognition. Because sensor data is stored with a time stamp, it represents a sensor’s state at a certain moment. This time stamping of data points implies that data never becomes less relevant over time, because it tells about a specific moment in time. During the interviews, data points losing relevance over time was not mentioned by any of the interviewees.

### 4.3.5. Use limitation

Within the PFIP, use limitation is defined as the limitation of access to data, so that it can only be used for its specific purpose. The connected concern is that collected information is used for another purpose as was intended. From the interviews, we see that sharing of data, selective sharing, and secondary use of data is connected to Use Limitation.

Many interviewees give aspects of use limitation in their definition of privacy. For example, DEV2 explains privacy as the ability to hide specific information from third parties:

“Mijn idee van privacy is het niet kenbaar maken van bepaalde informatie aan meestal derden.” (page 81) translates into: “My idea of privacy is not to reveal certain information to usually third parties.”

Whereas STAFF3 states that you should be able to control which information is available to others, and which is not:

“Controle over informatie en data die van jou beschikbaar zijn al dan niet beschikbaar zijn voor anderen.” (page 123) translates into: “control on information and data available about you and may or not may be available to others.”

Sense software enables users to share their data with others. Sense employees think that it is the personal responsibility of the user with whom they share their information. This is best shown in the following quote by DEV3:

“Daar heeft Sense niets mee te maken, als jij besluit om je data aan iemand te geven dan is het je eigen verantwoordelijkheid dat diegene er goede dingen mee doet” (page 93) translates into: “It is not Sense’s business, if you decide to give your data to someone, that is your own responsibility whether or not that person does good things with the data”

Using the collected data for another purpose as intended, may be a wish of third parties, as is seen in the following quote by STAFF3:

“Ik denk dat dat er bij sommige partners en bij sommige klanten de wens leeft om de data te gebruiken, ook al is die van eigen gebruikers.” (page 125) translates into: “I think that some partners and some clients wish to use the data, even though it belongs to the individual users.”

### 4.3.6. Reasonable security

The PFIP states that security should be applied where necessary, and more sensitive data needs better security measures. Not having enough protection of data is a fear described on the CFIP scale (section 2.3.2). Security measures most present in the interviews are encryption and depersonalisation of the data. Safety is a term also related to this principle.

The possibilities of encryption are stated by DEV1 as being a trade-off with system performance:

“Volgens mij was het idee om alle data te encrypten die de database in moeten, maar dat brengt een heleboel performance-issues met zich mee.” (page 75) translates into: “I think it was the idea to encrypt all data going into the database, but that brings a lot of performance issues.”

Depersonalisation of data can also increase the feeling of security. On this, STAFF1 states that it is important that data can not be traced back to the subject of the data:

“Het is in ieder geval voor mij belangrijk of het herleidbaar is tot mij.” (page 108) translates into: “It is certainly important to me if it is traceable to me.”

In general, security should provide (a feeling of) safety. DEV4 voices the wish that data is safe when stored at Sense, but is uncertain whether that is possible:

“Dat je data veilig is bij Sense. Ik weet niet of ik dat zou kunnen zeggen.” (page 102) translates into: “That your data is safe with Sense. I am not sure I could say that.”

#### 4.3.7. Accountability

Accountability is a principle present within PFIP, which states that record keepers can be held accountable for compliance with all of the other principles (section 2.3.2). Responsibility and consequences are the main terms found in the interviews which relate to accountability.

Security is most linked to accountability in the interviews. DEV3 states that security measures are not applied sufficiently at this moment:

“Op dit moment wordt het niet genoeg gedaan” (page 94) translates into: “At this moment, it is not done enough.”

DEV2 adds to that by stating that someone needs to have a look at security:

“Er moet gewoon iemand naar kijken” (page 88) translates into: “Someone has to look into it.”

Using the term someone, instead of a specific person or organisation, indicates that responsibility is not always clear.

DEV4 suggest that there should be consequences for not adhering to privacy principles when handling user data:

“Dat er consequenties tegenover kunnen staan als je daar niet goed mee omgaat.” (page 102) translates into: “That there may be consequences if you do not properly deal with it.”

#### 4.3.8. New: Individual ownership

The principles of privacy deal with data collected about a person. Within the definition it is not directly clear who owns the data. Sense employees voice the opinion that data belongs to the person whose data is collected. For this we use the term *individual ownership*. To illustrate *individual ownership*, DEV1 says it is logical that your data belongs to you:

“Het is logisch dat het jouw data is en niet die van een ander en dat jij daar zeggenschap daarover hebt.” (page 74) translates into: “It is logical that it is your data not another’s, and that you have control over it.”

However, STAFF3 indicates that some third parties claim ownership of the data, because they created the system with which the data is collected:

“Mensen denken ook op de een of andere manier dat de data van hun is, omdat zij misschien alleen het systeem gemaakt hebben waarmee het verzameld wordt.” (page 124) translates into: “People think in one way or another that the data is theirs, because they may have only made the system with which it is collected.”

#### 4.3.9. New: Company access denial

Next to determining which external parties can access user data, interviewees also voiced opinions on data access by Sense employees. Because *use limitation* states that data should only be used by authorized personnel, and Sense personnel might fall into this category, we define the expression *company access denial*. This expression deals with limiting access to data in such a way that Sense employees can not have access to data of a user.

At this moment, it seems that employees still have the possibility to access data, as voiced by STAFF2:

“Het lijkt er wel op dat wij toegang zouden kunnen krijgen.” (page 83) translates into: “It looks like we could get access.”

DEV4 has looked into the possibilities of access denial for employees of Sense, and says that this is near impossible to achieve:

“Dat het wel lastig is om het zo af te schermen dat wij daar als Sense-medewerkers daar bij zouden kunnen. Het is onmogelijk om dat zo af te schermen” (page 103) translates into: “That it is difficult to protect it so that we as employees at Sense could not access it. It is near impossible to screen that off.”

### 4.3.10. Conclusion

Based upon the interviews, a total of seven expressions is used, of which two not found in the literature. The two expressions, *collection limitation* and *data quality*, found in literature are left out of consideration for representing the brand identity of Sense Observation Systems (Sense). *Collection limitation* does not apply to the case of Sense, because relevance of collected data is not always clear at the moment of collection. *Data quality* is left out, because the type of data collected informs on the state of a person at a particular moment so it will remain relevant over time. Both new expressions (*individual ownership* and *company access denial*) are added to the considered expressions for Sense's brand identity because respondents indicated these expressions to be part of their definition of privacy. The entire list of expressions and pictorial representations used in the remainder of this report is represented in table 4.1.















Aspect	Observed keywords	Icons (+/-)
Openness and transparency	transparency, (clear) communication	 
Individual participation	change, deletion	 
Collection limitation	n/a	-
Data quality	n/a	-
Use limitation	(selective) sharing, secondary use	 
Reasonable security	encryption, depersonalisation	 
Accountability	responsibility, consequences	 
Individual ownership	ownership, data is yours	 
Company access denial	access, company, government	 

Table 4.1: *Privacy aspects* with pictorial representations used in this report.

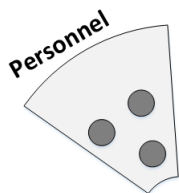
## 4.4. Exploration of identity types

This section describes the different *identity types* and the beliefs on privacy present therein as obtained through the interviews, where we explored each identity type found in the conceptual model (section 3.1). Each identity type is described in its own subsection which concludes with a punctualisation of the like-minded actors for a clear analysis of the entire network in chapter 5.

### 4.4.1. Personnel identity

For personnel, the way in which they experience influence from one another is explored in the first part of this subsection. After explaining the inter-personnel network of influence, the beliefs on privacy therein are discussed in the second part. Punctualisation of this identity type is then performed based upon the findings in the first two parts.

#### Actors



Respondents were all asked to name the three Sense employees with whom they had the most contact. Answers to this question are represented in the network shown in fig. 4.2. Each respondent is given a number indicating their strength in influencing others. The strength is indicated by the amount of times a respondent is named by others as influencer. A total of 3 is subtracted from this number to compensate for people influencing the respondent. The resulting number is positive when someone influences more people than he the amount who influence him, and is negative when it is reversed. The influencer's strength is 0 when he influences as many people

as influence him.

In the interviews, Sense's manager (strength +4) clearly came out as a highly influential individual, connecting to all others within the network. Both Almende employees do experience contact with Sense employees, but are not among the most important for those employees. Each and every Sense employee influences and is influenced by at least one other Sense employee. A

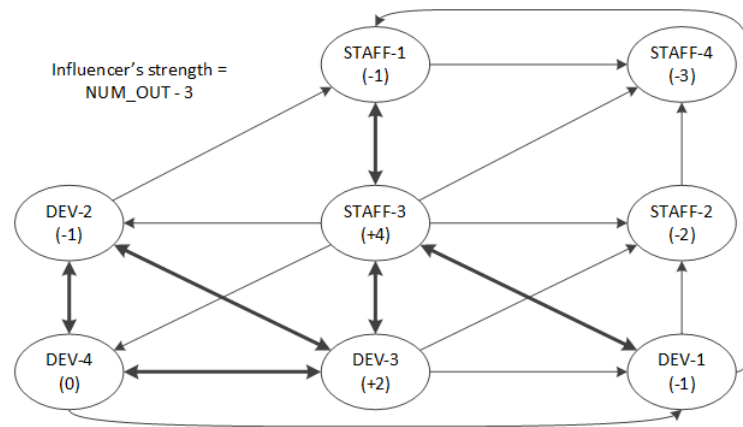


Figure 4.2: Inter-personnel influence network of all interviewed employees. Arrows originate from an employee named as a top-3 contact by the employee toward whom the arrow points. The influencers strength is determined by the amount of arrows going out minus the three arrows coming in. For this network with 8 actors the influencer strengths could range from +4 (highly influential) to -3.

notable observation is the cluster of developers in the bottom-left of the network. These three employees (DEV-2, 3, and 4) all influence one another and form a clique in that sense. When looking at the network, it seems that DEV-3 can be seen as a bridging connection between STAFF-3 on one side and DEV-2 and DEV-4 on the other. DEV-3 also has a high strength of influence, even the highest within the developers cluster.

### Privacy

Beliefs on the definition of privacy differ per respondent. However, the concept *use limitation* (🔒) was present in each person's definition. Each employee expressed that it is part of data privacy that data collected on you should not automatically be available to everyone. STAFF3 expresses this as follows:

“Wat telt is dat niet zomaar iemand bij je data moet kunnen” (page 124]) translates into: “What matters is that not just anyone should be able to access your data.”

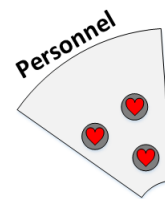
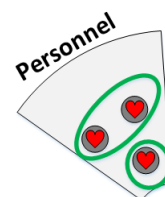


Figure 4.3 shows that there is no clear segment within the influence-network, in terms of management or developers, where beliefs on privacy are more pronounced. However, the difference between those who do and do not have a broad idea on the definition of privacy is clearly visible. Half of the respondents relate only two principles to privacy, of which one is *use limitation*. The other half of the respondents also expressed *individual ownership* (👤), and furthermore three of them expressed *openness and transparency* (🔍) or *individual participation* (👤). These respondents indicate data on a person belongs to that person, that end-users should be able to know what data is collected on them, and next to this, they say end-users should also be able to edit, or even remove data related to them. All members in a role of management are aware that privacy also means that reasonable security measures should be taken to protect data from unauthorized access. Two Sense employees mention that *accountability* (📋) is required to make end-user privacy work. There is no consensus regarding the necessity of *company access denial* for privacy because it is confirmed (🔒) by two employees and contradicted (🔓) by two others.

### Punctualisation

Because of the diversity in response obtained from interviewed employees, the Actual Identity regarding personnel will be punctualised into two separate clusters. The first cluster contains employees limited in their expression of privacy, and will be defined only by the presence of *use limitation* (🔒) as a principle of information privacy. This first cluster is called *selective* and consists of DEV-1, DEV-3, STAFF-1, and STAFF-4. The second cluster contains employees who also have voiced that *openness and transparency* (🔍),



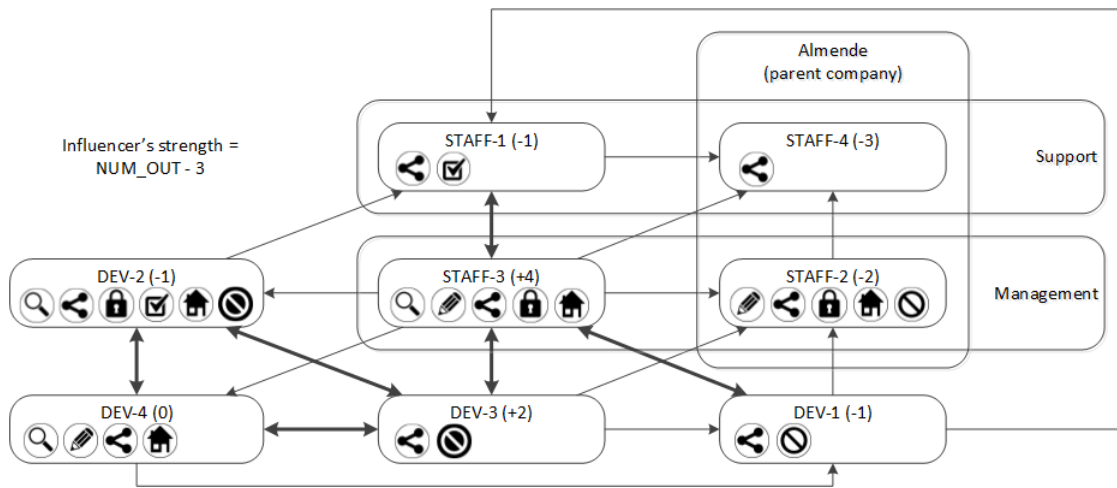






Figure 4.3: The distribution of beliefs on privacy throughout employees of Sense

*individual participation* , and *individual ownership*  are part of information privacy. Because reasonable security was also voiced by 3 out of the 4 in this group, this principle is also added. Members of this *extensive* cluster are DEV-2, DEV-4, STAFF-2, and STAFF-3. *Company access denial* , and *accountability* , are not linked to any of the employee clusters, because they were not mentioned by the majority of all interviewees, or the respondents in a specific cluster. The summary of privacy aspects per cluster is given in table 4.2.








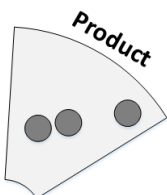
Cluster							
Selective			+			+	
Extensive	+	+	+	+		+	

Table 4.2: Expressions for privacy in the *selective* and *extensive* clusters within the *personnel identity*.

### 4.4.2. Product Identity

The products developed at Sense, are all related to one another, and also embody principles of information privacy. In the first part of this subsection, the relations and structure found through the interviews are discussed, followed by the distribution of principles of privacy. This subsection concludes with the punctualisation of the product portfolio based upon privacy principles found within products.

#### Actors



Software developed by Sense uses a self-developed server-infrastructure called the backend. This backend runs on a database which is an off the shelf product. Some products communicate directly with the backend, such as CommonSense, and the MiriaNed test setup. However, most products use the Application Programmers Interface (API) to communicate with the backend. These products can be divided into three groups of products: Home-brew apps (developed for and by Sense), Almende apps (for companies under the Almende umbrella), and third party apps (developed for external customers). Figure 4.4 visualises the structure of the software developed by Sense and privacy values found therein, as given in the interviews.

#### Privacy



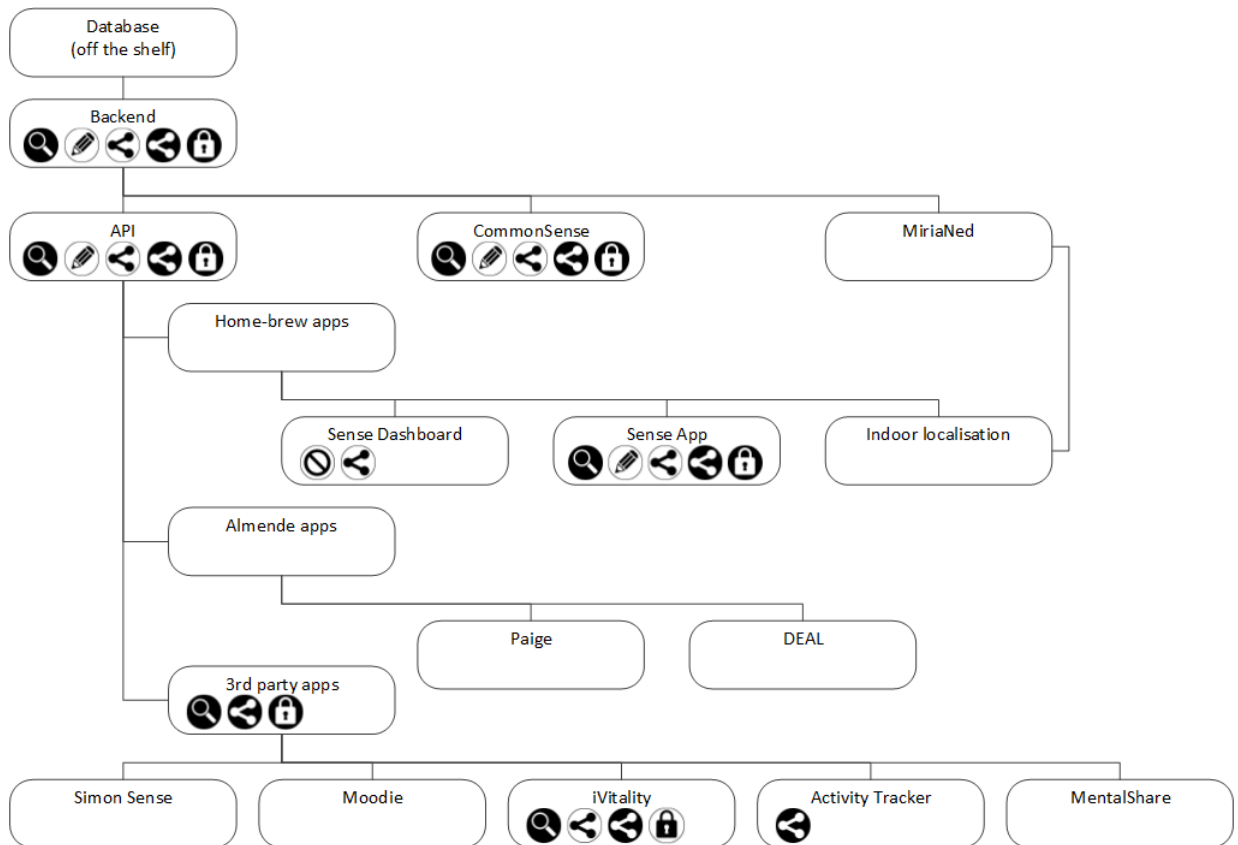
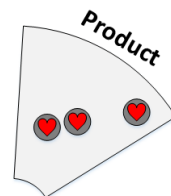


Figure 4.4: The distribution of beliefs on privacy throughout products (co-)developed by Sense

In general, the interviews tell us that Software developed by and for Sense, values the *individual participation* of end-users. Users are technically able to share their data with whom they want. However, the following comment by DEV-3 indicates that the implementation of Sense’s vision on privacy is a bit lacking:

“Zoals het bij Sense een beetje gaat, eerst zeggen dat we het kunnen, en het dan pas maken. Zo is dat nu ook met privacy.” (page 96) translates into: “As it goes at Sense, first we say we can do it, and only then we start to make it. As it is now with privacy.”



This comment is in line with earlier findings from Lahlou et al. [18], who indicated this gap between vision on privacy and implementation of this vision. There are efforts made by Sense to implement the vision in the software, which have various amounts of success.

Openness and transparency on how to set and revoke these rights of sharing are not implemented very thoroughly. DEV-2 states that it is only visible that you share your data, not with whom:

“dat je deelt. Niet met wie je deelt” (page 88) translates into: “that you share. Not who you share with”

The security of data stored at the Sense database is at this moment quite minimal according to employees. The present safety measures are quite uniform according to STAFF-3, no distinction in encryption is made between storing a person’s heart rate or a local weather forecast.

“In de basis is de databeveiliging redelijk uniform.” (page 127) translates into: “The basis of the data security is quite uniform.”

According to DEV-3, security issues are due to ignorance, not unwillingness:

“Het is niet door onwil, dat de beveiliging slecht is, ..., maar door onkunde.” (page 95) translates into: “It is not through unwillingness, that security is bad, ..., but through incompetence.”

Next to this, also no one in the company seems to be right on top of the security issue. This indicates a lack of *accountability* 🛑. As told by DEV-2:

“Daar zit niet iemand bovenop” (88) translates into: “Nobody is on top of that.”

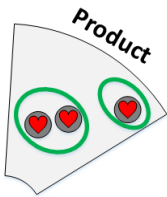
Regarding company access denial, DEV-2 states that it looks like employees can access collected data when they wish to:

“Het lijkt er wel op dat wij toegang zouden kunnen krijgen.” (page 83) translates into: “It looks like we could get access.”

Some projects by Sense have proven to be more successful than others in implementing good privacy practice. According to employees, the new Sense Dashboard is a good example of how to give end-users more insight and control over their data. DEV-3 explains that privacy should be dealt with correctly, if Sense wants to go public:

“Dashboard is iets wat wij helemaal zelf hebben gebouwd en daarbij is managen van privacy een belangrijke feature. Want als we Sense een keertje aan de mensen beschikbaar willen maken, moeten we de privacy goed hebben.” (page 95) translates into: “Dashboard is something we have built from scratch and wherein managing privacy is an important feature. If we want to make Sense available to the people sometime, we must have good privacy measures.”

### Punctualisation



From the interviews, the general impression is that Sense software contradicts *openness and transparency* 🗉, *reasonable security* 🛡️, and *accountability* 🛑. However, *individual participation* 🗑️ and *use limitation* 🗑️ is technically possible in the back-end of the software. Due to lacking visibility in the user interface, these features do not reach the end-user properly. Recent developments, such as the Dashboard product, have taken a step into adoption of the privacy vision. Here *openness and transparency* 🗉, *individual participation* 🗑️, and *use limitation* 🗑️ have been implemented more thoroughly. It should be said that this is a project started by Sense, and

without the requirements of a client.

Because of the recent developments, we divide the products of Sense into two clusters (*old* and *new*) shown in table 4.3. In both these clusters, we contradict *reasonable security* 🛡️, *company access denial* 🗑️, and *accountability* 🛑. In the *new* cluster, *openness and transparency* 🗉, *individual participation* 🗑️, and *use limitation* 🗑️ is present, while the *old* cluster contradicts *openness and transparency* 🗉. We leave *individual participation*, and *use limitation* out for the *old* cluster, because of the lack of visibility and implementation thereof in most of the old products.

Cluster	🗉	🗑️	🗑️	🛡️	🗑️	🏠	🛑
Old	-			-	-		-
New	+	+	+	-	-		-

Table 4.3: Expression for privacy in the *old* and *new* clusters within the *product identity*.

#### 4.4.3. Communicated Identity

Sense communicates to potential clients and software developers through several media. In the first part of this subsection, the classifications of different media found through the interviews are discussed. Distribution of privacy principles are discussed and accompanied by examples from the interviews in the part thereafter. This subsection concludes with the punctualisation of the communication means based upon found privacy principles.

### Actors

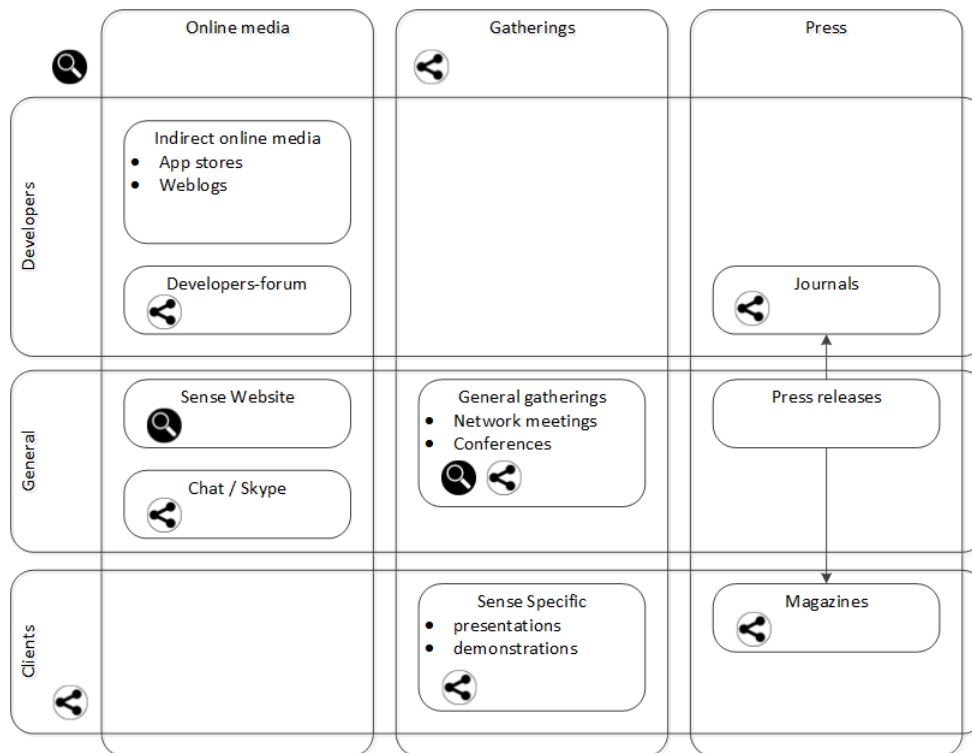
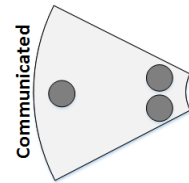


Figure 4.5: The distribution of beliefs on privacy throughout Sense's communicated identity. The horizontal axis shows different media whereas the vertical axis shows different target audiences.

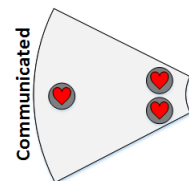
Sense has a corporate website, and web pages dedicated to specific products. Press releases are used to reach journals and magazines which are mostly technology-minded. Conferences and network meetings are used as a means to present Sense to potential clients who are further introduced to Sense by demonstrations and presentations. These can take place at either Sense's office, a location of the clients' choosing, or even through teleconferencing. Developers indicate to have contact with third party developers, who make use of their API, through a Sense-owned developers-forum and weblogs. Figure 4.5 visualizes the different means used to connect with clients and developers, and privacy values found therein.



### Privacy

The respondents indicate that external stakeholders often voice a fear of "big brother"-like practices on initial contact (DEV1 on page 71 and DEV4 on page 101), which enforces the relation between ubiquitous computing and privacy described by Heersmink et al. [12]. DEV-3 indicates that Sense does not initiate communication on the topic of privacy:

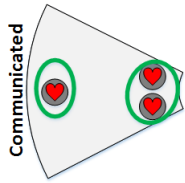
"We hebben het er zelf meestal niet over, meestal andere mensen." (page 94) translates into: "We usually do not talk about it, mostly other people."



This lack of *openness and transparency* on privacy within the communicated identity is further backed up by STAFF-3, who states that privacy is not represented properly on the website and other communication means:

"Op sommige pagina's wel, maar representatief niet. Te weinig." (page 127) translates into: "On some pages, but not representative. too little."

### Punctualisation



Within the *communicated identity* of Sense, *openness and transparency* ☹️ seems lacking; the intention of Sense is not directly clear, which is expressed by the 'big-brother'-comments by visitors of conferences. *Use limitation* ☹️ is an aspect which is often voiced by Sense employees through informing clients that their software can be used to choose with whom you share your data. The lack of *openness and transparency* ☹️ is seen as generally present throughout the identity by respondents, and the communication of *use limitation* ☹️ is connected to more than half of the actors found in the *communicated identity*. Other aspects of privacy were not mentioned in the interviews. We therefore punctualise the *communicated identity* into one point which has the belief of *use limitation* ☹️, and the negated aspect of *openness and transparency* ☹️, as is visualized in table 4.4. For readability purposes, the actors clustered within the *communicated identity* are represented as the *media cluster*.

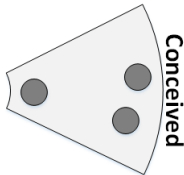
Cluster	🔍	✍️	🔄	🔒	☑️	🏠	🚫
Media	-		+				

Table 4.4: Expressions for privacy in the *media cluster* within the *communicated identity*.

#### 4.4.4. Conceived Identity

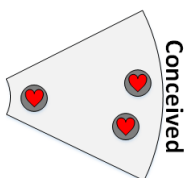
The communications and projects of Sense involve several external stakeholders, which make up the *conceived identity*. The diversity of stakeholders indicated during the interviews, makes privacy beliefs of individual organizations less reliable due to lack of response on these organizations. Therefore, *privacy aspects* are directly mapped to stakeholder-groups instead of individual organizations.

##### Actors



An important external stakeholder group is the Almende Group. These companies are family to Sense, and Sense has developed a firm relationship with them. The main market which came to mind during the interviews is related to healthcare, which is indicated as an important market by 6 out of 8 respondents. The fact that Sense is a spin-off of the research oriented company Almende, is still seen in the group of companies in the field of research and development, which is mentioned by 4 out of 8 employees. Besides whole fields of interest, individual projects were also mentioned, which are left out of consideration. Categories of individuals such as end-users, software developers, and visitors of the website, are taken into account. An overview of the mentioned groups and how privacy is distributed amongst them, is found in fig. 4.6.

##### Privacy



The beliefs on privacy at the sibling companies of Sense are indicated to be similar to what is the general thought at Sense. We indicate this with the attributes *openness and transparency* ☹️, *use limitation* ☹️, and *individual participation* 🗳️.

The field of healthcare is a field where professionals deal with sensitive data on the health of their clients. STAFF-1 points out the responsibility that Sense has for this sensitive data; it should not get into the open:

“jij als degene die omgaat met de gegevens van de patient moet zorgen dat die gegevens niet zomaar op straat terecht komen.” (page 107) translates into: “as the one handling patient data you have to take care that data does not end up on the street.”

STAFF-3 even deems the security measures taken for healthcare a bit extreme, and thinks that they apply a procedure mostly to prevent any future legal actions:

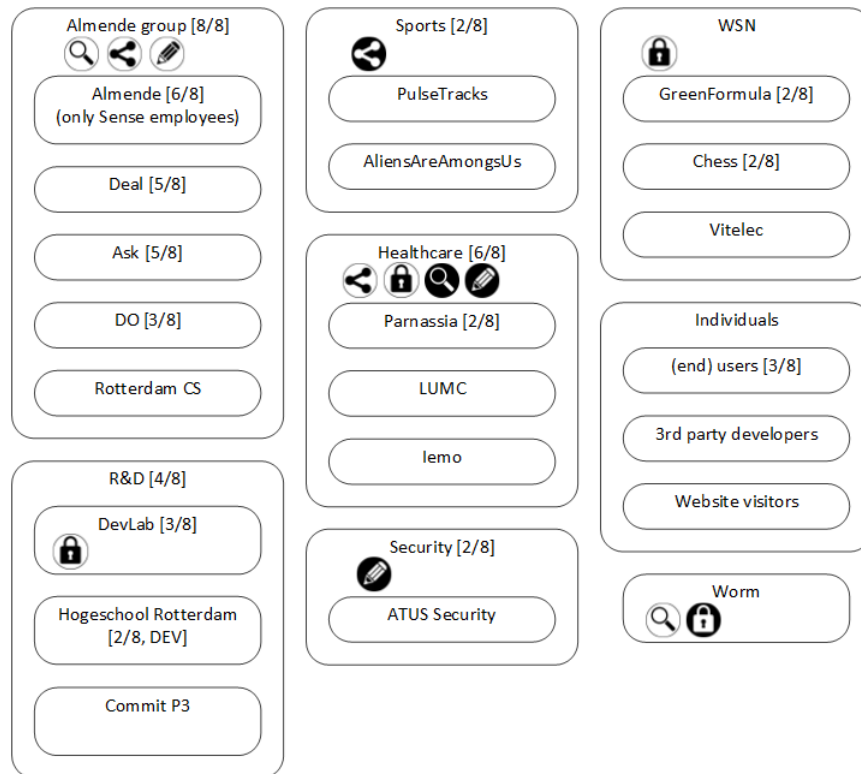


Figure 4.6: Distribution of beliefs on privacy throughout Sense's *conceived identity*

"Vaak zie je dat ziekenhuizen daar ook niet heel erg rationeel in zijn, maar een soort 'cover your ass'-procedure hanteren" (page 125) translates into: "It is often seen that hospitals are not quite rational but they apply a sort of 'cover your ass'-procedure."

We therefore associate healthcare with the aspect of *reasonable security* 🔒, and *use limitation* 🔄.

We do not link *individual ownership* to the *conceived identity*, because of the indication by STAFF-3 who says that third parties claim ownership of the data, because they created or paid for the system with which the data is collected:

"Mensen denken ook op de een of andere manier dat de data van hun is, omdat zij misschien alleen het systeem gemaakt hebben waarmee het verzameld wordt." (page 124) translates into: "People think in one way or another that the data is theirs, because they may have only made the system with which it is collected."

We extend this to the entire *conceived identity* and connect the contradiction of *individual ownership* 🗑️ to the *conceived identity*. STAFF-4 informs that clients often have no feeling for the idea of *individual ownership*. STAFF-3 furthermore thinks that some clients wish to use the data which is actually property of the end-user:

"Ik denk dat dat er bij sommige partners en bij sommige klanten de wens leeft om de data te gebruiken, ook al is die van eigen gebruikers." (page 125) translates into: "I think that some partners and some clients wish to use the data, even though it belongs to the individual users."

We associate this with the negation of *use limitation* 🔄 by these customers. However, these same customers often voice "big brother"-fear during first contact with Sense, as indicated by DEV-4:

"dan hebben ze het idee dat het een monitoring systeem is dat helemaal niet voor de gebruiker ten goede komt, maar voor iets anders." (page 101) translates into: "they have the idea that it is a monitoring system with no benefit to the user, but for something else."

This contradiction, and the overprotective attitude of healthcare towards data collection, might indicate that there is a broad range of beliefs within the *conceived identity*. The stakeholders found in this *identity type* might also be ill informed about the possibilities and ethics of handling end-user data.

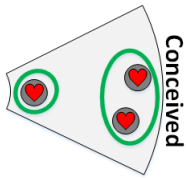
Other groups, such as R&D, Sports, and Wireless Sensor Networks, were not extensively labeled with aspects of privacy. STAFF-1 tells that end-users for the sports sector have a high drive to share their accomplishments with the world which is associated with more *openness and transparency* ☺, but also a lack of need for *use limitation* ☹:

“Binnen de sport, mensen die gebruik maken van dat soort dingen hebben ontzettend behoefte aan mededelingsdrang.” (page 107), translates into: “within sports, people who use those kind of things [sports apps] have a tremendous communication urge.”

According to DEV-2, Researchers are often not keen on dealing with end-user privacy, their first concern is obtaining data, and privacy is a second order problem:

“Hun eerste belang is gewoon die data en hoe dat met privacy zit is een gewoon een tweede orde probleem.”(page 84) translates into: “Their first concern is simply the data and how privacy is handled is just a second order problem.”

### Punctualisation



We reduce the variety of external stakeholders to three *clusters* deemed representative based upon the interviews. The *clusters* are named *Almende*, *health*, and *sports* as can be seen in table 4.5. The *Almende* cluster consists of Sense’s siblings, and its parent company Almende. They roughly represent the same privacy values as Sense personnel: *openness and transparency* ☺, *use limitation* ☹, *individual participation* ☺, *individual ownership* 🏠, and the neglect of *accountability* ☹.

*Health* represents the healthcare sector, and others who are keen to keep the data collected to themselves. The privacy values connected are: *use limitation* ☹, *reasonable security* 🛡, the contradiction of *individual ownership* 🏠, and contradicted *openness and transparency* ☹. *Sports* is formed by groups who do not have privacy as priority, such as the before mentioned stakeholder groups sports and research. We link *openness and transparency* ☺, and the contradiction of *use limitation* ☹ to this cluster. *Company access denial* is not associated with any of these clusters because it was not mentioned during interviews.

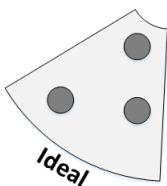
Cluster	☺	☹	☺	🛡	☺	🏠	☹
Almende	+	+	+		-	+	
Health	-		+	+		-	
Sports	+		-				

Table 4.5: Expressions for privacy in the clusters *Almende*, *health*, and *sports* within the *conceived identity*

#### 4.4.5. Ideal identity

The ideal identity represents the strategic position of a company within its market. Internally this identity is steered by the corporate strategy. External entities related to this identity consist of competitors in the market, and of regulators and legislation.

### Actors



Strategic choices of Sense are made in a yearly meeting. Each employee is present during this meeting in which the management shows the progress and achievements of last year, as well as the projects planned for the coming year. Employees are asked to name the achievements of which they are most proud, and the pitfalls of last years projects. The meeting ends with writing down the possible goals to reach in the next year, which are then clustered

and assigned to different employees. Other than a picture being made of the lists, the strategy is not documented. Several employees mentioned that the company's policy is quite ad hoc, such as DEV-3:

"Het beleid wat er nu ligt, is nogal ad hoc." (page 92) translates into: "The current policy is quite ad hoc."

STAFF-4 assumes there is not much difference between the corporate strategy and the vision of the management, which is found in the desired identity.

Regulators and legislations play no role of significance, according to management. It is a problem which is tackled when encountered, which is not the case yet. DEV-3 and DEV-4 assume that laws and regulations do not steer Sense's strategy. As DEV-4 puts it:

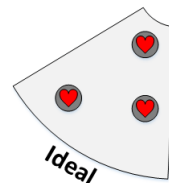
"ik denk niet dat die heel sturend zijn" (page 99) translates to: "I do not think these are very directing"

Available technology steers Sense, because it enables new options for their products. The providers for this technology consist of telephone manufacturers, and reach Sense through the interfaces found in the operating systems on these telephones. At the moment Sense develops software on Android and iPhone. Competition for Sense is found in the field of *internet of things*, which develops software to collect and aggregate all kinds of sensor data. Sports apps which read out sensors on smart phones are considered competition. The main competitors voiced during the interviews are OpenSense, Pachube (first rebranded to Cosm, later to Xively), Dysi, and MapMy\* (sports).

### Privacy

We assume the company strategy to be in line with the vision of the management, as expressed in the *desired identity*. The legislators appear to have no direct influence on Sense, but are usually concerned with limiting the spreading of data. STAFF-3 says laws are dealt with only when necessary:

"Dat is een typisch geval van cross the bridge when you get there." (page 127) translates into: "That is a typical case of cross the bridge when you get there."



*Use limitation* is connected to this concern. DEV-3 assumes that competitors such as OpenSense and Cosm are further developed in terms of privacy implementation. However, competitors usually have little nuance on the area of *use limitation*. As told by STAFF-3:

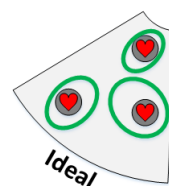
"Je hebt vaak weinig mogelijkheid tot nuance of gradaties waarin je iets deelt of niet deelt" (page 125) translates into: "You often have little possibility of nuance or gradations wherein you either share or you don't."

According to Sense employees, they furthermore lack *openness and transparency* regarding the use of collected data. And DEV-4 tells that administrators at competing companies always have access to the data:

"Als admin kan dat [toegang tot de data krijgen] wel. Ik ken geen partij die dat niet zo heeft. (page 100)" translates into: "As admin it [getting access to the data] is possible. I know of no party who does not have that option."

### Punctualisation

The *ideal identity* represents the best place for the company, given its market. The corporate strategy is not documented very thoroughly and is present mainly in the minds of the personnel, and the *desired identity*. We therefore leave the company strategy out of the punctualisation. Rules and regulation steer towards *use limitation*, whereas competition lacks the nuance on that aspect. *Use limitation* ↔ is therefore seen as an aspect which



places Sense on a unique location in the market, and we therefore place it in the ideal identity. *Openness and transparency* is an aspect lacking in products of the competition. We therefore also place *openness and transparency* ☹ in the *ideal identity*. Because competitors provide access to the data for their own administrators, denying them access gives a competitive advantage in the field. We therefore add *company access denial* ☹ to the ideal identity. Other aspects of privacy were not extensively linked to either legislators, or the competition. The punctualised ideal identity therefore contains the aspects *openness and transparency* ☹, *use limitation* ☹, and *company access denial* ☹. This punctualisation is represented in table 4.6.

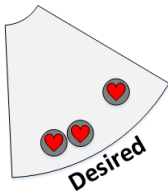
Cluster	☹	☹	☹	☹	☹	☹	☹
Market	+		+				+

Table 4.6: Expressions for privacy in the *market* cluster within the *ideal identity*.

#### 4.4.6. Desired identity

Balmer and Greyser [3] state that the *desired identity* “lives in the hearts and minds of corporate leaders”. We therefore take the vision of Sense as stated by STAFF-2 and STAFF-3 as basis for the *desired identity* (as visible in fig. 4.7). Next to that, the perceived corporate vision expressed by the other employees is also considered.

##### Privacy



The vision of Sense’s top management covers all aspects of privacy defined in table 4.1. Quotes associated with these aspects are shown below. Sense’s management wishes to have some exemplary cases to show the values of privacy. We see this as the aspect *openness and transparency* ☹. STAFF-3 also expects that this helps in battling the ‘Big Brother’-type fear expressed by potential clients:

“Op het moment dat je ze een voorbeeld laat zien hoe je de data wel gebruikt, maar dat dat alleen kan als je dat deelt, dan geeft dat misschien vertrouwen dat er op de achtergrond niks anders gedaan wordt. Als je helemaal niks doet met de data, worden mensen achterdochtig.” (page 125) translates into: “The moment you show them an example of how you are using the data, but that it is only possible if you share it, then that might be give confidence that there is no secret agenda. If you do not do anything with the data, people get suspicious.”

STAFF-2 states that users should be able to change their data, with the exception of data covered by a certifying organisation (such as is the case with your home adress):

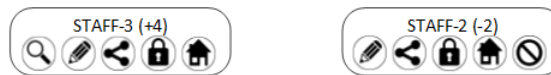
“Alle data moet je kunnen veranderen behalve als je een gecertificeerde instantie hebt.” (page 120) translates into: “You should be able to change all data, unless there is a certified organisation.”

This is connected to the aspect *individual participation* ☹. Related to *individual ownership* ☹, STAFF-2 and STAFF-3 share the vision that the data is not only changeable by the user, but also property of the same user of whom the data is collected. As STAFF-2 puts it:

“De data is van jou dan mag je het dus ook veranderen, je mag het deleten, je mag er vanalles mee doen wat je wilt. Je mag hem mooier maken. Het is jouw data” (page 121) translates into: “The data is yours, you can also change it, you can delete it, you can do whatever you want with it. You can make it nicer. It’s your data.”

According to STAFF-2, users should also be able to undo the sharing of their data. He states that this is technologically challenging, and not that common:



Figure 4.7: Distribution of beliefs on privacy throughout Sense's *desired identity*

"Ze [gebruikers] moeten kunnen ontscharen als het even kan. Dat is ook een technologisch uitdagend ding. Dat komt nog niet zoveel voor" (page 111) translates into: "They [users] should be able to de-share were possible. This is technologically challenging. This is not done very much."

The vision of the management on data security is further than technically achieved at the moment. STAFF-2 finds that data should be protected even from the government, which relates to the aspect of *company access denial* ☹ :

"Je moet er zeker van zijn dat men er niet bij kan en die moet in zekere zin niet alleen beschermd worden tegen anderen, maar ook tegen de staat." (page 111) translates into: "You should be sure that they can not reach it, and it should be protected against others in some way, also against the state."

STAFF-2 also mentions a method related to the aspect of *accountability* ☑ . In an example of an electronic patient dossier for healthcare, he recommends to register each time someone accesses the data and looks into the file. He says it is not bad to look into such files, as long as you do not mind that your visit is noted:

"Het is helemaal niet erg dat je kijkt, maar je moet wel even laten zien dat je kijkt." (page 118) translates into: "It is not bad that you look, but you need to show that you look."

#### Punctualisation

Both managers responsible for the vision of Sense according to the employees named all of the aspects of privacy present in this research. We therefore represent the *desired identity* as one cluster containing every aspect of privacy defined in section 4.3.10, as can be seen in table 4.7. The actor clusters within the *desired identity* is named *vision*, because it represents the vision of the management.



Cluster	🔍	✍	🔄	🔒	☑	🏠	🚫
Vision	+	+	+	+	+	+	+

Table 4.7: Expressions for privacy in the *vision* cluster within the *desired identity*

#### 4.4.7. Brand Identity

During the interviews, participants were asked what they want to promise the world if they were Sense. The answers provide insight into the preferred aspects of privacy for the brand identity, or brand promise. As seen in table 4.8, The aspects *use limitation* ☹ and *reasonable security* 🔒 were both named by seven respondents in their preferred brand promise. Four of the respondents answered that *openness and transparency* ☹ or *company access denial* ☹ should be part of the brand promise. *Individual participation* ✍, *accountability* ☑, and *individual ownership* 🏠 were voiced by less than half of the respondents.

#### 4.4.8. Conclusion

Ten clusters were defined in this chapter to represent the corporate network which influences the brand identity, and are found in table 4.9. The responses given for the preferred brand identity are found in table 4.8.








Cluster							
Covenanted	4	2	7	7	0	3	4

Table 4.8: The occurrence of aspects of privacy in responses for the preferred brand identity. Numbers indicate how many respondents linked the aspect to their preferred brand identity.

Identity	Cluster							
Personnel	Selective			+			+	
Personnel	Extensive	+	+	+	+		+	
Products	Old	-			-	-		-
Products	New	+	+	+	-	-		-
Communicated	Media	-		+				
Conceived	Almende	+	+	+		-	+	
Conceived	Health	-		+	+		-	
Conceived	Sports	+		-				
Ideal	Market	+		+				+
Desired	Vision	+	+	+	+	+	+	+

Table 4.9: Privacy aspects connected to clusters found in identity types

## 4.5. Conclusion

The clusters displayed in table 4.9 are used as input for the network analysis performed in chapter 5, where each of the privacy aspects are tested for stability based upon the systems theoretical approach by van der Vorst [31]. Chapter 5 tests the feasibility of each of the aspects mentioned by respondents without looking at frequency, whereas chapter 6 also takes the occurrence of each of the aspects amongst company employees in consideration as an indicator for feasibility.

# 5

## Network alignment analysis

In this chapter we visually analyse the suitability of different privacy aspects as core concepts in the *brand identity* of Sense. Section 5.1 first recapitulates the *privacy aspects* and *actor clusters* found throughout the actor network. Section 5.2 briefly explains how *privacy landscapes* help in the alignment analysis of privacy aspects. Section 5.3 analyses each of the privacy aspects expressed in the interviews using the identity landscape-method. Section 5.4 concludes the chapter with a summary of the analyses.

### 5.1. Network recapitulation

The *privacy aspects* evaluated in this chapter originate from the interviews as described in section 4.3. The list below shows the seven aspects with a set of keywords defining the aspect and the icon used throughout this thesis.

**Openness and transparency** 🔍 secret records, perception, communication, transparency

**Individual participation** ✎ access by data subject, editing, deletion of data, change

**Use limitation** ↻ use, authorized personnel, data release, (selective) sharing, secondary use

**Reasonable security** 🛡 security, encryption, sensitive data, protection, depersonalisation

**Accountability** ☑ compliance, record keeper, responsibility, consequences

**Individual ownership** 🏠 ownership, data is yours

**Company access denial** 🚫 restricted access, company, government

The *actor clusters* shown in this chapter originate from the interview results described in section 4.4. From the interviews, ten clusters are defined within the six *identity types* defined in the conceptual model (section 3.1). The clusters are defined as follows, with the *identity type* between parentheses:

**Selective (Personnel)** Personnel limited in their expression of privacy.

**Extensive (Personnel)** Personnel with a wide range of expressions related to privacy.

**Old (Products)** Products from the beginning of Sense, includes Sense's backend systems.

**New (Products)** Newer products of Sense, showcasing the possibilities of acquired data.

**Media (Communicated)** All means of external communication used by Sense.

**Almende (Conceived)** Sense's siblings and parent company Almende.

**Health (Conceived)** Healthcare sector and others keen to keep collected data to themselves.

**Sports (Conceived)** External stakeholders not the most interested in privacy.

**Market (Ideal)** Best place for Sense in the market according to perceived qualities of the competition.

**Vision (Desired)** Sense's vision as in the minds of the management (STAFF-2 and STAFF-3).

The position of the actors clusters on each of the privacy landscapes described in this chapter are based upon the expressions of privacy as summarized in table 4.9 and according to the process described in section 3.5 which is summarized in section 5.2.

## 5.2. Privacy landscapes

This chapter focuses on the link strengths between the brand identity and other identity types. For increased clarity, we leave any other connection out of the visualisations used in this chapter. For each privacy aspect described in section 5.1, a visualisation is created showing the links to each of the actor clusters. In the example shown in fig. 5.1, the privacy aspect under review is placed in the middle of the privacy landscape.

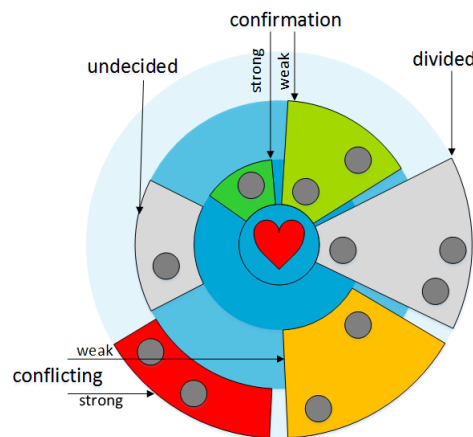


Figure 5.1: different configurations of the surface of *identity types*

The actor clusters are placed on one of the three rings according to their confirmation or contradiction of the central aspect. actor clusters confirming the privacy aspect under review are placed on the inner ring, whereas contradicting actor clusters are placed on the outer ring. Actor clusters for which no attitude towards the central aspect was found are placed on the ring in between the other two.

The stability of each identity type on the landscape is visualised by adapting the surface of the identity type to the clusters placed thereon. Therefore, the *identity type's* surface shape is reduced in size as long as it still spans the entire set of clusters within it. This method results in six possible configurations of the *identity surfaces*, as can be seen in fig. 5.1. The top two configurations (green) show a positive (confirmation) link to the central concept, whereas the bottom two configurations (red) show a negative (conflicting) link to the central concept. The remaining two configurations are either *undecided* when no clear expression on the value is found in the *identity type*, or *divided* when both *confirming* and *conflicting* values are found.

## 5.3. Analysis

This section shows the *identity landscapes* constructed for each of the seven privacy aspects using the method described in section 5.2. Each *identity landscape* shown in fig. 5.2 is accompanied by a description, and recommendations on where to focus attention to improve alignment to the central privacy concept of that *privacy landscape*.

### 5.3.1. Openness and transparency

Taking the privacy aspect of openness and transparency as a core concept in the brand identity yields the network as shown in fig. 5.2a. We see that the ideal and desired identity are both very close to the centre of the image, illustrating that these identity types relate to the aspect of openness and transparency. Within the personnel identity we see that the two clusters have a different link to the aspect of openness and transparency. The extensive cluster relates to the aspect, but the *selective cluster* is undecided. This makes the personnel identity a bit less focused compared to the ideal and desired identity. The communicated identity is quite focused, but contradicts the aspect of openness and transparency. The product and conceived identity have no clear focus on the aspect of openness and transparency. They both have clusters which confirm, and which contradict the aspect. This makes these identity types less focused. In total, the privacy landscape contains 3 actor clusters with a contradiction link to the aspect of openness and transparency.

### 5.3.2. Individual participation

The aspect of individual participation provides a privacy landscape as found in fig. 5.2b. Here, the desired identity again shows a confirmation link towards the aspect of individual participation. Within the personnel, product, and conceived identities, some clusters are undecided about the aspect. However, there are no contradictions to individual participation in any of these three identities. The ideal and communicated identity are both undecided about the aspect. Note that not one of the identity-clusters has a contradiction type link to individual participation.

### 5.3.3. Use limitation

The privacy landscape for use limitation is given in fig. 5.2c and shows quite some focus towards the aspect of use limitation. The desired, ideal, communicated, and also personnel identity are focused towards the centre of the landscape. This shows both focus and confirmation for the aspect of use limitation. The product identity features an undecided and a confirmation cluster, making this identity less focused, but still giving a positive attitude towards use limitation. The conceived identity has clusters with confirmation and contradiction links, and is therefore considered undecided. In total, one cluster in the entire landscape shows a contradiction link.

### 5.3.4. Reasonable security

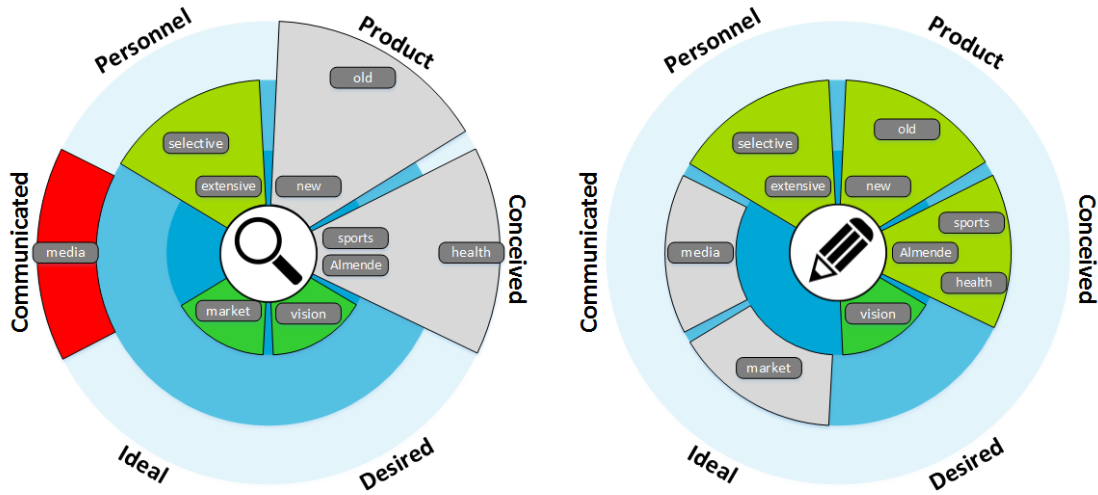
The privacy landscape for reasonable security is given in fig. 5.2d and shows diversity in link types. The desired identity is focused and confirms the aspect of reasonable security. Both the personnel and conceived identities have a general confirmation of the aspect. However, they also contain some undecided clusters; the extensive cluster within the personnel identity and the health cluster within the conceived identity, show a outspoken confirmation of the aspect. The ideal and communicated identities are focused with an undecided link. The product identity shows a focused and contradiction link to reasonable security.

### 5.3.5. Accountability

As seen in fig. 5.2e, *Accountability* shows a diversity of link types. The *desired identity* is focused and confirms the aspect of *accountability*. Three *identity types* show a focused yet undecided link with the aspect: the *ideal*, *communicated*, and *personnel identity*. The *conceived identity* has a contradiction link with *accountability* while the *Almende* cluster draws towards contradiction and *sports* and *health* are undecided. The *product identity* is strongly focused on the contradiction link.

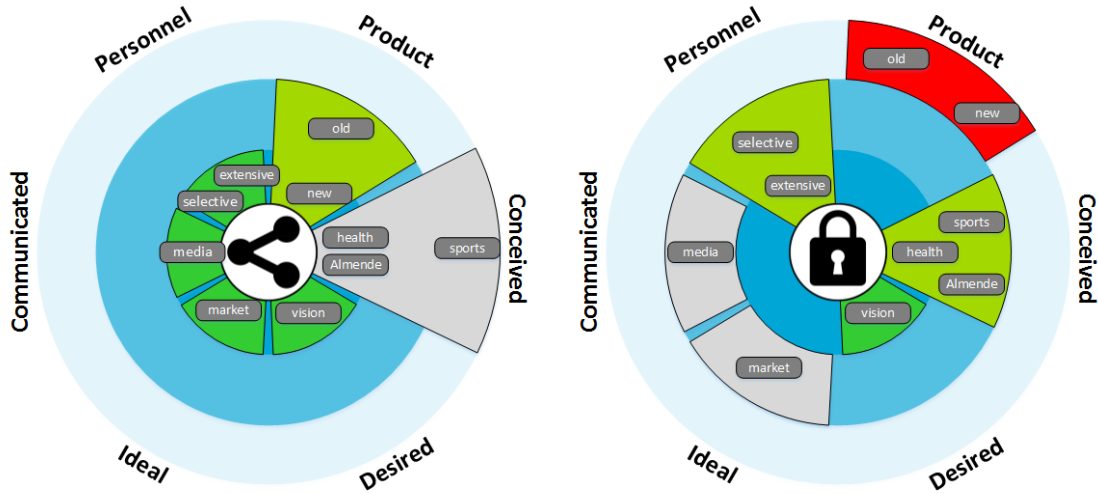
### 5.3.6. Individual ownership

Individual ownership shows a quite diverse privacy landscape which is shown in fig. 5.2f. The *personnel* and *desired identity* have a confirmation link to the central aspect of individual ownership. Three identities have an undecided link to individual ownership: the *product*, *communicated*, and *ideal identity*. The *conceived identity* has an divided link where the *health* cluster contradicts the aspect of individual ownership and *Almende* confirms the aspect.



(a) Openness and transparency

(b) Individual participation



(c) Use limitation

(d) Reasonable security

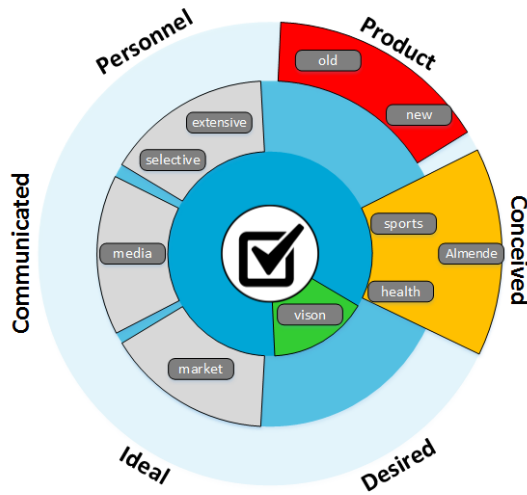
Figure 5.2: Privacy landscapes of the seven analysed privacy aspects

### 5.3.7. Complete access denial

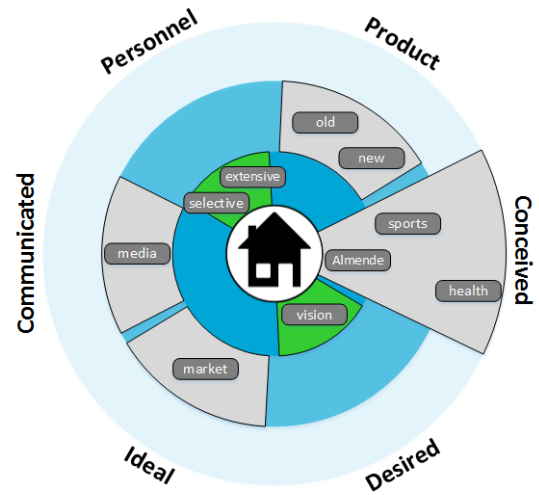
Complete access denial also shows a quite diverse privacy landscape, as is shown in fig. 5.2g. The *ideal* and *desired* identities have a focused and confirmation link to the central aspect. Three identities show an undecided link to complete access denial: the *personnel*, *communicated*, and *conceived* identity. The *product* identity shows a focused contradiction link to complete access denial, mainly due to the statements made regarding the technical difficulty or impossibility of denial of access to all users except the provider of the data him- or herself.

## 5.4. Conclusion

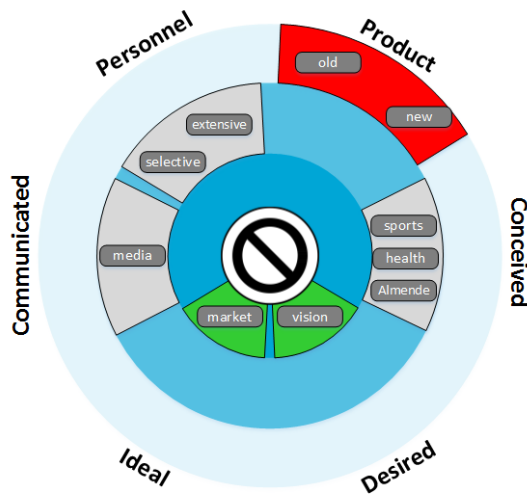
The *privacy landscapes* discussed in this chapter provide an overview of suitability for each of the *privacy aspects* found in the interviews. The *landscapes* show a variety of configurations, from those where each *identity type* links to the central *aspect* (e.g. *use limitation*) to those where only the *desired* identity links to the central *aspect* (e.g. *accountability*). Variety is also seen in the amount of *identity types* that touch the outer ring of the landscape, where the *conflicting* link-type is located; *Individual participation* has no *identity types* with a *conflicting* link-type, whereas *openness and transparency* has three *identity types* touching on the outer ring of the landscape.



(e) Accountability



(f) Individual ownership



(g) Complete access denial

Figure 5.2: Privacy landscapes of the seven analysed privacy aspects (continued)

This visibility of differences makes that the *privacy landscapes* give a useful overview for the advice in [chapter 6](#).



# 6

## Brand management advice

This chapter advises the company Sense on how to get their vision on end-user privacy into their brand identity as a core concept. The advice should be seen as an interpretation of the results from chapter 4 and chapter 5. Section 6.1 defines which privacy aspect is best suited as a core concept in Sense's brand identity. Section 6.2 introduces the concept of frames of reference from van der Vorst [31] and applies them to the suited privacy aspect. We describe a set of actions on how to strengthen the concept in order to make it more central in section 6.3. In section 6.4 we advise on which privacy aspects can be added to the core concept so as to strengthen it further. Section 6.5 covers the points of attention for other privacy aspects found during our research. In section 6.6 we state our conclusion.

### 6.1. Privacy aspect selection

The selection of privacy aspects as a core concept for the brand identity is based upon stated preference of the employees and analysis of the identity landscapes. Section 4.4.7 shows that the aspects *use limitation* and *reasonable security* were both named by seven respondents in their preferred brand promise. Other aspects were preferred by four employees at most. A generally confirming privacy landscape for *use limitation* is seen in fig. 6.1. With only two actor clusters not confirming the aspect, it is the most confirming landscape found in the analysis in chapter 5. The privacy landscape for *reasonable security* shows a contradiction link for the product identity because of concerns voiced for appropriate data security in Sense products. Artefacts such as products are rigid elements within an actor network [22] and require substantial effort to change. Because of the contradiction link to products in the landscape for *reasonable security*, and the generally confirming privacy landscape for *use limitation*, this advice focuses on the privacy aspect of use limitation.

### 6.2. Frame of reference

In the context of Sense, *use limitation* embodies the sharing of data, selective sharing thereof, and prevention of secondary use. This is also seen in the quote by STAFF3 found in section 4.3.5:

“Controle over informatie en data die van jou beschikbaar zijn al dan niet beschikbaar zijn voor anderen.” (page 123) translates into: “control on information and data available about you and may or not may be available to others.”

van der Vorst describes 3 frames of reference through which a core concept in the brand identity can be expressed: taxonomic (product properties), feature (functional features), and metaphorical (symbolic features) [31, p. 192] (see also section 2.3.4). These frames of reference help van der Vorst to bind on different levels of abstraction. Because the *brand identity* covers more than the products found within the *product identity*, we advise to use a frame of reference that is broader than product properties. Because product properties are used in the taxonomic frame of reference, we reject it as an option.

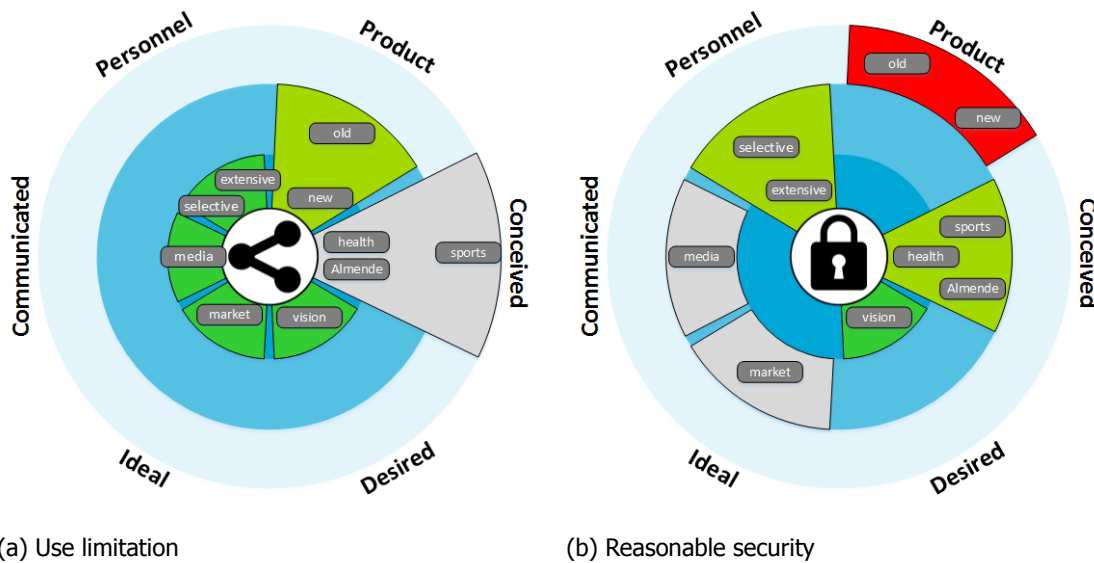


Figure 6.1: *Privacy landscapes* for the *privacy aspects* preferred as core concept by the respondents. Each of these aspects was mentioned by seven out of the eight respondents

Application of a feature frame of reference embodies functional features, which can be shared by more than the developed products. van der Vorst [31] gives 'safe' as example of a feature frame of reference and indicates that a wider variety of products can share this feature (e.g. bicycles, aeroplanes and even clothing can be referred to as 'safe'). We believe this amount of variation suffices for Sense's product domain in the field of data collection, interpretation, and sharing. We think that a feature frame of reference is therefore a viable option. *Use limitation* as a privacy aspect is already a functional feature, but could receive more emphasis when used as a core concept. An example of a positive approach to *use limitation* as a feature frame of reference is 'selective sharing', as stated in a personal conversation with the CEO of Sense (July 3th, 2014). An example of a corporate slogan using this feature frame of reference is:

"Sensible information sharing"

van der Vorst [31] gives 'security' (related to the feature reference 'safe') as example of a metaphorical frame of reference. The link to products which is present in a feature frame of reference is less directly visible in symbolic features used in a metaphorical frame of reference. Using symbolic features makes it easy to embed *use limitation* into identity types other than the *product identity*. An example of a symbolic feature based upon *use limitation* is 'conversation'. An example of a corporate slogan using this metaphorical frame of reference is:

"Conversations that make Sense"

Symbolic features can cover multiple functional features and are therefore preferred when more *privacy aspects* are added to the core concept. The choice for which frame of reference to use, and what terminology is best, is up to the company itself. This also depends on whether or not other privacy aspects are added to this core concept, so as to broaden it. Suggestions for broadening the concept are given in section 6.4. Where broadening the concept is an optional step, we do strongly advise to strengthen the concept by developing the suggested means as explained in section 6.3.

### 6.3. Actions for brand management

From the interviews, it is clear that documentation of core concepts is mostly lacking; the privacy aspects are in the minds of employees. To ensure a more enduring core concept as advised by Albert and Whetten [1], we advise to use artefacts which are more rigid in an actor network [22].

We propose the use of a corporate slogan, development of a showcase product, development of a market strategy, and expression of the corporate vision. The identity types on which these means have an assumed effect are shown in table 6.1. Many of the means encourage stabilisation over time for the actor network surrounding the *brand identity*. Most of the suggested means require no intensive guidance of a communication manager and we expect that they can be developed by Sense internally. A communication professional could help in developing a corporate slogan or write down the corporate vision.

Means	Affected identity types
corporate slogan	communicated, personnel, desired
showcase product	product, conceived, personnel
market strategy	conceived, ideal
corporate vision	desired, communicated

Table 6.1: Brand management means linked to their affected identity types

In the *personnel identity*, we found a favourable attitude towards *use limitation* in both definition of privacy and preference for use as concept in the brand identity. Frequent exposure to the core concepts of the corporate brand can ensure that they are remembered. A corporate slogan, present in the visual brand identity is a good option with which to increase this exposure.

The *product identity* shows the *old*-cluster sporting an unknown link to *use limitation*. This is mainly due to the user being unable to see with whom exactly his data is shared. If a user has selected multiple parties to share his data with, this is not clearly visible within the user interface. To obtain a confirmation link to *use limitation*, this cluster needs to improve on insight into the parties with whom the data is shared. According to the respondents, the *new*-cluster already provides this needed insight. Development of a product showcasing the possibilities of *use limitation* to potential clients, can help to attract clients with comparable values, as well as provide Sense's developers with more experience with the concept.

For the *communicated identity*, it is important to let correspondence express the core concepts of a brand's identity. Ideally all communication breathes the corporate values in a variety of abstractions so as to make exposure both conscious and subconscious. The earlier mentioned corporate slogan would be a good starting point for expressing the corporate values. The communicated identity reaches both employees and external stakeholders. An example of this is Sense's participation in conferences where employees represent the company to potential clients.

To ensure alignment of the *conceived identity* with its stakeholders, a screening of clients would be advisable. The showcase product can help in self selection amongst potential clients; some of whom will not be impressed by the technical features Sense's products offer in relation to *use limitation*. However a client selection based on the corporate values, ensures strengthening of the brand identity. Such a selection is not necessarily per client, but can also take the form of a market strategy describing in which markets Sense wants to develop. Thereby selecting markets that best fit the corporate values. Respondents indicated The healthcare-sector is an example of a promising market where the aspect of *use limitation* is a high priority, thus confirming the company values.

The *ideal identity* also benefits from the development of a market strategy because it consciously places Sense in the market, thereby marking the territory Sense wishes to develop in. In this way competitors can be better defined based upon comparison of corporate values. However, *use limitation* makes up only one of the corporate values of Sense.

The *desired identity*, and more specifically the vision of Sense, seemed to be distributed quite well throughout the interview respondents. However, a written down version of the corporate vision could be beneficial. An outspoken vision helps to communicate the core values such as *use limitation* to multiple stakeholders. Writing down the corporate vision of the management helps employees to see what the purpose of the company is, and external stakeholders to better trust the company's intentions.

## 6.4. Aspects adding to the concept

The proposed core concept can be broadened by adding related privacy aspects. As explained in section 6.2, this enables Sense to use a more metaphorical frame of reference, and also prevents too much emphasis on one specific technical feature in the brand identity. We see opportunities in the use of the aspects *individual participation*, *individual ownership*, and *openness and transparency*. These opportunities are briefly motivated below.

*Individual participation* deals with the change and deletion of personal data by the user. In the practice of Sense, intelligent algorithms enable the user to develop their own derivative data sets. This enables the user to only share that which is really of interest to the one they share with, without giving away anything else. This aspect therefore gives users more control on what they share. Because *use limitation* is about selective sharing of data, Sense's take on *individual participation* strengthens the core concept.

The aspect *individual ownership* focuses on the ownership of personal data and states that this is property of the person on whom the data was collected. This aspect relates to one of the core values of the parent company Almende, which is an advocate of self-organization: organization without central control. Acknowledging that the data collected on an individual is owned by that same individual, facilitates that this person can decide with whom to share his or her data. Therefore, we believe that this privacy aspect can further strengthen the core concept.

Finally, the aspect *openness and transparency* is related to the availability of information about data collections on a person, to that person. When Sense provides users with clear information on the data sets available on their person, this enables them to make better informed choices on what data to share with whom. We therefore believe that this aspect can be used to strengthen the core concept.

These aspects can fit the 'conversation'-metaphor as stated by in conversations with STAFF2 and STAFF3. We shall briefly explain how the mentioned *aspects* can possibly be linked to the chosen metaphor. For example, people can tell whatever they want in conversation, they can even lie (*individual participation*). Whether or not they want to engage in conversation, is up to them (*use limitation*), and their thoughts are theirs (*individual ownership*). Sense will not listen in on these conversations (*openness and transparency*).

## 6.5. Other considerations

Besides the possibilities of the immediate choices of strengthening or adding to the concept, there are a couple of other considerations to be made: the decay of the concept strength over time, and how to deal with the unused aspects of privacy.

When the core concept is developed according to the advice in previous section, the brand needs to be managed in order to keep its distinctiveness and centrality. Distinction of a brand based upon the core concept becomes threatened when other brands take on the same core concept. Centrality of a brand is threatened whenever new entities are added to the set of influencing actors; personnel rotates, new products are developed, and markets or clients change. Each of these actions is a possible threat to the centrality of the brand. It is therefore essential to make the core concepts of Sense known to the changing actors involved in the brand. A reminder to the core concepts can be developed in a corporate slogan, so as to help keep the core values in mind and associated with the brand.

Each of the privacy principles defined by Westin [33] is part of the generally accepted definition of privacy. It is advisable to implement these principles in the products of Sense. The analysis of *privacy aspects*, shows that the principles of *reasonable security*, and *accountability* are generally neglected. Because this thesis focuses on the development of a fitting core concept, we left these *aspects* out of further consideration, however the design principles found in the historical overview by Iachello and Hong [14] might help in developing these *privacy aspects*. We assume that it benefits the overall privacy ethic to put effort on the implementation of these *principles*.

## 6.6. Conclusion

As discussed within this chapter, we advise to use the *privacy aspect* of *use limitation* as core concept within the *brand identity* of Sense. This advice is an interpretation of the thorough ex-

plorations and analysis based upon the conceptual model found in chapter 3. We propose to strengthen this core concept through the use of a corporate slogan, development of a showcase product, development of a market strategy, and expression of the corporate vision. To prevent a focus on technical implementations, *use limitation* can be supported by the *privacy aspects individual participation, individual ownership, and openness and transparency*.



# 7

## Conclusion, discussion, and future work

This chapter concludes the research performed in this thesis. Section 7.1 answers the sub questions posed in section 1.3 as well as the main question of this work. Section 7.2 presents a reflection to the process, results, general applicability, theory, and practice. Section 7.3 concludes this chapter by presenting options for future work based upon the reflections on the research.

### 7.1. Conclusion

The conceptual model developed in chapter 3 was used to find an answer to each of the sub questions. We believe this conceptual model to be a proper answer to the main research question because of this. This section goes through each of the sub questions to explain how they were answered, and ends with the answer to the main research question.

#### 7.1.1. SQ1: Which entities determine Sense's corporate brand?

Based on theory relevant to brand management, we found an answer to sub question 1 through interviews. The AC<sup>3</sup>ID-model by Balmer and Greyser [2] was expanded to accommodate for the apparent gap between thought of privacy present in the minds of employees and the implementation of privacy measures in software products [18]. Our model defines six identity types linked to the brand identity in which entities (both human and non-human) reside. A general indication of entities found for each identity type is as follows:

**Personnel** employees, management

**Product** products, services

**Communicated** corporate communication, media and press, (external) events

**Conceived** partners, clients, prospective clients

**Ideal** competitors, policy makers, legislators, strategy

**Desired** (top) management, vision

Based on the responses on the interviews, we defined ten distinct *clusters* of entities related to Sense's brand identity. These *actor clusters* as discussed in chapter 4 included individuals, organizations, websites, and products. The entities were grouped by similarity in privacy-vision and the following clusters were defined to show which entities determine Sense's corporate brand. The identity types for the clusters are placed between parentheses:

**Selective (personnel)** employees limited in their expressions on privacy

**Extensive (personnel)** employees with a wide vocabulary on privacy

**Old (product)** large amount of Sense's products including its back-end systems

**New (product)** small cluster covering more recent Sense products

**Media (communicated)** including online media, conferences, and press media

**Almende (conceived)** Sense's siblings, and its parent company

**Health (conceived)** organizations keen on keeping data access restricted

**Sports (conceived)** organizations interested in sharing achievements with the world

**Market (ideal)** competitors, legislators, defining the ideal place in the market

**Vision (desired)** Sense's top management

### 7.1.2. SQ2: How are principles on end-user privacy present within those entities?

From theory on both end-user concerns about privacy (CFIP [25]), and software design principles on privacy (PFIP [33]), we developed one list of privacy aspects in which both these sources [25, 33] are linked. The privacy aspects and corresponding indicators were defined as follows:

**openness and transparency** informing, secret records, perception

**individual participation** access by subject, editing, deletion

**collection limitation** purpose for collection, excessive collection

**data quality** relevant, up-to-date, errors over time

**use limitation** use, authorized personnel, data release, purpose for use

**reasonable security** security measures, encryption, sensitive data, protection

**accountability** compliance, record keeper

These privacy aspects were used to guide the interviews. During the interviews, it was found that two aspects (*collection limitation* and *data quality*) out of the original seven were not relevant to the business of Sense. Also, two new aspects (*individual ownership* and *complete access denial*) related to privacy were added to the list. The indicators of the aspects were updated based upon the interviews. This resulted in the following list of privacy aspects, iconic representation thereof, and corresponding indicators :

**Openness and transparency** 🔍 secret records, perception, communication, transparency

**Individual participation** ✎ access by data subject, editing, deletion of data, change

**Use limitation** ↶ use, authorized personnel, data release, (selective) sharing, secondary use

**Reasonable security** 🛡 security, encryption, sensitive data, protection, depersonalisation

**Accountability** ✅ compliance, record keeper, responsibility, consequences

**Individual ownership** 🏠 ownership, data is yours

**Company access denial** 🚫 restricted access, company, government

The privacy aspects were used to label the views on privacy expressed for the entities which determine Sense's brand identity. After clustering the entities, this resulted in a labelled set of the ten before mentioned clusters as shown in table 7.1. This table shows how privacy principles are believed to be present within the entities surrounding the corporate brand.



Identity	Cluster	🔍	✎	🔗	🔒	✅	🏠	🚫
Personnel	Selective			+			+	
Personnel	Extensive	+	+	+	+		+	
Products	Old	-			-	-		-
Products	New	+	+	+	-	-		-
Communicated	Media	-		+				
Conceived	Almende	+	+	+		-	+	
Conceived	Health	-		+	+		-	
Conceived	Sports	+		-				
Ideal	Market	+		+				+
Desired	Vision	+	+	+	+	+	+	+

Table 7.1: Privacy aspects connected to the clusters found in identity types. A plus (+) shows a confirmation link between the aspect and the cluster, whereas a minus (-) shows a contradiction link. Where no sign is shown, the link type is unknown.

### 7.1.3. SQ3: How can principles on end-user privacy become central in Sense's corporate brand ?

The works of Balmer and Greyser [2] and van der Vorst [31] form the basis for the answer to sub question 3. We believe that a central element in a corporate brand is one which is present throughout the actor network which makes up the brand. To find a privacy aspect fitting this definition, we developed the privacy landscape visualisation of the actor network in relation to the corporate brand. We also believe that a corporate brand should be supported by the employees of a company to make it work. We therefore also asked the employees for their preference regarding an element in the corporate brand related to privacy.

Out of the seven defined privacy aspects, *use limitation* and *reasonable security* were preferred by seven out of eight employees. From these two privacy aspects, the privacy aspect *use limitation* was deemed the best option because of its generally confirming attitude throughout the actor clusters, which is shown in fig. 7.1.

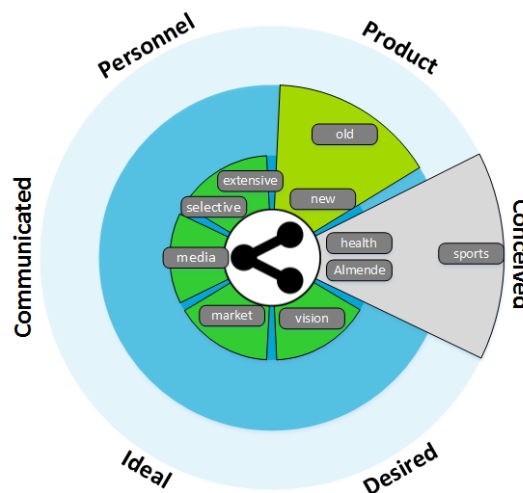


Figure 7.1: Privacy landscape for *use limitation*. Only the actor clusters *old* and *sports* are not directly confirming the aspect *use limitation*. Actor clusters near the centre show a confirming attitude towards the central privacy aspect

We believe that privacy principles can become more central in the brand identity through focused effort on, or rejection of the actor clusters away from the centre. In the case of *use limitation*, we advised to put effort into the *old* cluster in the product identity by development of a showcase product, be aware of the lack of alignment between Sense and their clients in

the *sports*-cluster, and to consider the development of a market strategy fitting the values of the company.

#### 7.1.4. SQ4: How to manage a brand identity based upon these principles?

For stabilisation of the actor network regarding the concept of privacy, we proposed to use a corporate slogan, development of a showcase product, development of a market strategy, and expression of the corporate vision. This mix of means is assumed to affect the identity types as stated in table 7.2. Most of the proposed means do not require the intensive aid of Almende's communication manager, and are therefore assumed manageable by Sense internally. However, for the development of a corporate slogan, we advised to work closely with a communication professional. We believe to have answered sub question 4 thoroughly with the given advice and its coverage of each identity type related to the brand identity.

Means	Affected identity types
corporate slogan	communicated, personnel, desired
showcase product	product, conceived, personnel
market strategy	conceived, ideal
corporate vision	desired, communicated

Table 7.2: Brand management means linked to their affected identity types

#### 7.1.5. Main research question

This research has found an answer to each of the sub questions defined in section 1.3, and is therefore able to answer the main research question:

How to manage the corporate brand of Sense Observation Systems so as to encompass the principles on end-user privacy present within the corporation?

## 7.2. Discussion

### 7.2.1. Reflection on the process and result

In this subsection, we first evaluate the process: literature survey, selection of respondents, and interpretations made upon the collected data. After the process-evaluation, we conclude with an analysis of the general reliability and validity of the research, and how they could be approved.

#### Literature survey

The literature survey for this research was carried out through application of the methodology developed by van der Sanden and Meijman [30]. Search clusters were created that are related to the main research question which were used to search for literature using the Scopus database. As more of the search clusters were combined, more relevant literature was found. Most of the literature was found through this method and this structured search was seen as a useful tool for future literature surveys. We have made some observations regarding our execution of the literature survey:

- The work of van der Vorst [31] did not originate from the structured search. Because of its relevance to the search-clusters "corporate branding" and "networks", this source was found to be relevant to this work.
- Not all search clusters were related to the research question in this report, which might have influenced the relevance of the obtained works. However, the literature used to develop the conceptual model (chapter 3) is selected from a relevant set of results and the primary sources found for Actor-Network Theory, AC<sup>3</sup>ID, and privacy were all cited by multiple of the relevant works.

- The use of only the Scopus database might have caused bias in the results. Falagas et al. [8] concluded that Scopus covers more journals as compared to Web of Science in their comparison of Scopus, Web of Science, PubMed, and Google Scholar. They also mention that Google Scholar is mostly useful for helping to find the most obscure information, but has a use marred by inadequate, less frequently updated, citation information. PubMed is a database for medical research, and was therefore not useful for the literature survey. We believe that by use of the Scopus database, we accessed the best database available to our research.

### Selection of respondents

The selection of respondents was limited to actors from the *personnel* and *desired identity*. The assumption of Gioia et al. [10] is followed that company employees can estimate the beliefs of external stakeholders. This assumption can lead to a projection bias, where respondents think that other actors share their beliefs on privacy. However, the *privacy landscapes* shown in the network analysis show a variety in beliefs on privacy throughout the various identity types; respondents were especially critical on the products developed by the company itself. The fact that all *privacy aspects* have a confirmation link to the vision of the management (see table 7.1), shows that the *brand identity* on privacy originates at management level, as is indicated during interviews. For a better quantification of this projection bias, cross-validation of the obtained results is required.

### Interpretation of interview data

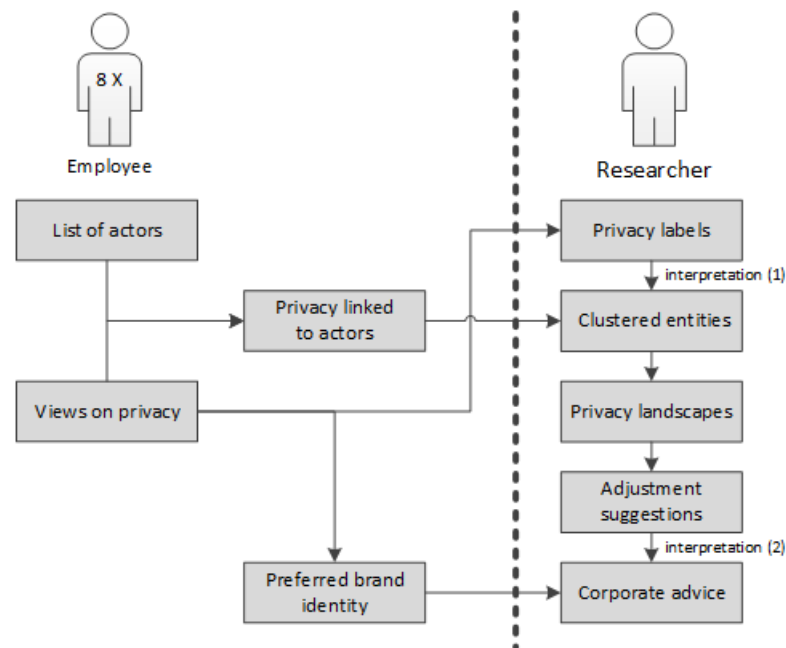


Figure 7.2: Steps taken in the formation of the privacy landscapes. The transfer from data (input from the employees) to information (privacy landscapes) is shown. Notice the two points (1,2) where the researcher makes an interpretation to move from one state to the other.

Figure 7.2 shows an overview of the information obtained from the interviews, and how this information is transformed. Because of the influential role of the researcher in the interpretation of the interview results, bias might have been introduced during post-processing:

1. Semi-structured interviews require labelling of the data, which can result in observation bias.
2. The results of combining multiple observations into one actor-network might be biased by the opinion of the observer.
3. Contradicting beliefs on one actor can only be represented as positive or negative towards a *privacy aspect*.

4. Clustering multiple actors and defining the *privacy aspects* related to the cluster may introduce observation bias.

With the amount of respondents (8) in this research, the combination of multiple observations by the researcher to make one actor-network can be replaced by a collaborative-session in which all respondents collaborate on developing the actor-network for Sense. During such a session, the beliefs on privacy for each of the actors in the network can be discussed and determined by the respondents. The steps of data transformation in such a process are shown in fig. 7.3. This change in methodology helps deal with the concerns mentioned above. To keep respondents uninfluenced on their own beliefs on privacy, individual interviews can be conducted prior to the group-session. However, we believe that in determining the brand identity, this step does not have the highest priority. It is more important to obtain an overview of the entire landscape, and obtaining individual opinions on privacy would re-introduce observer bias.

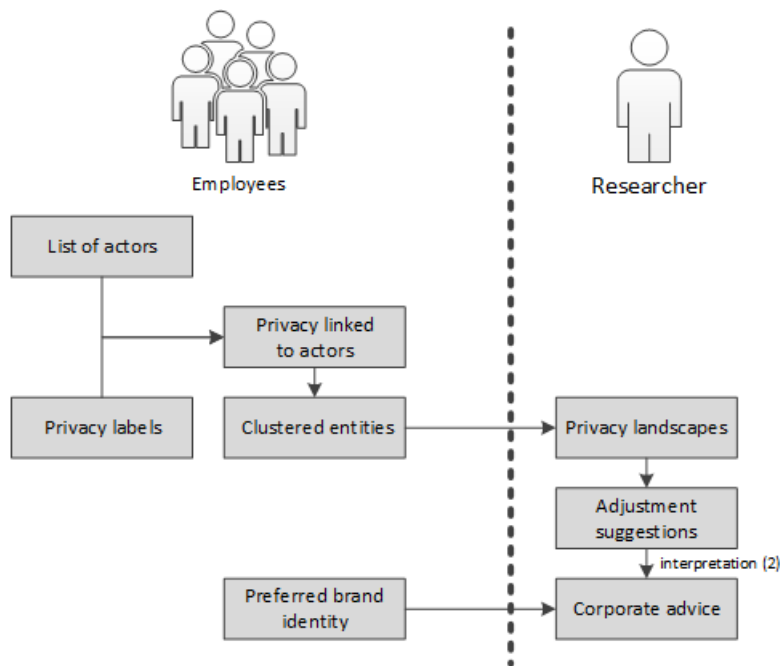


Figure 7.3: Improvement of the steps taken in the formation of the privacy landscapes. Compared to fig. 7.2, the interpretation used to create the actor clusters is moved to the side of the employees. Also, the individual interviews are replaced by a group session in which the employees co-create a representation of the actor network with connected privacy labels. The interpretation (2) used to develop a corporate advice remains

### Reliability and validity

In conclusion to the reflections in this subsection, we discuss the reliability and validity of the search for related work, the developed conceptual model, and the advice given to the company.

We believe the method used to find literature related to the research question as presented in chapter 2 is reliable because of its structured approach for determining relevance of literature. The structured approach reduced the influence of the researcher performing the search. Validity of the search was influenced by the inclusion of search terms ('trust') related to an earlier version of the research question. Because all search terms related to the final research question were also included, we assume the influence of this one set of search terms had no significant influence on validity.

Reliability of the applied conceptual model could be increased by removing observer influence where possible. In the current process, there is much interpretation of interview results by the interviewer, as seen in fig. 7.2. Figure 7.3 shows an improved process which removes much of the observer influence. Because the questions in the semi-structured interviews originate from the AC<sup>3</sup>ID-model, and theories on privacy, we believe that the conceptual model succeeds in

obtaining answers relevant to the research question. The used privacy landscape provides insight in the distributions of attitudes towards different privacy concepts and thereby remains focused on the research question. We therefore conclude that we have developed a valid conceptual model.

### 7.2.2. General applicability of the concept

In the introduction to this thesis, the general context of branding was sketched as a study in complexity. The development and application of the conceptual model was a study in which this complexity was captured, and the resulting privacy landscapes provided insight into the applicability of each of the aspects of privacy. This subsection discusses the general applicability of the results obtained in this research. The conceptual model was developed specifically to (1) be applied to Sense Observation Systems in order to (2) examine aspects of privacy to be used in (3) their brand identity. In this subsection, we explore how the conceptual model can be applied to (1) other companies, (2) other core concepts, and (3) other identity types.

#### Other companies

The conceptual model was applied to a small software company. Other companies have different actors involved in the identity types connected to their brand identity. The conceptual model can be applied to other companies because the model itself does not define a set of actors. However, the size of a company can be of influence to the application of the conceptual model. In a larger company, the larger group of internal respondents can have both positive and negative effects. A positive effect is that the confirmation of values appointed to actors through multiple respondents, which places more certainty on the resulting *landscapes*. A negative effect is that more different actors may be mentioned by respondents, implying more influence of the observer when interpreting and clustering the responses. The influence of the researcher on data interpretation and clustering should be minimized before applying this conceptual model to larger companies. Results from group discussions instead of individual interviews makes this possible for small groups of respondents. For such sessions, groups of at most 8 respondents would be best suited, but a well designed cooperative process could combine results from different groups in order to include a total of 40 to 80 participants [28].

#### Other identity types

The developed conceptual model is applicable to companies looking for a suitable brand identity. Because Balmer and Greyser [2] show the AC<sup>3</sup>ID-model as a *complete graph*, where all identity types are connected to one another (see fig. 2.1), we believe it is possible to switch the central location of the brand identity with other types. By doing so, it is possible to explore different identity types, and actors that would best fit the identity landscape. However, we do believe that the brand identity is best used as a focal point to the landscape because it is by definition “the synthesis of all identity types”[16].

#### Other core concepts

We analysed the viability of *information privacy* as a core concept for a brand identity. Step 3 of the conceptual model (see section 3.3) describes the *privacy aspects* and needs to be altered when the conceptual model is to be applied on another concept. The rest of the developed method requires that valuations of the chosen concept can be compared to one another. More specifically, the operationalisation of a chosen concept should make it comparable to what the actors *believe* about it. If this requirement is met, we believe it can be applied using the developed conceptual model.

### 7.2.3. Reflection on practice

In this subsection, we reflect on the practical aspects of the research in this thesis. We describe what we encountered within the company and also how communication professionals could benefit from the developed method.

#### Stable elements

One of the remarkable observations from the interviews was the apparent lack of enduring elements in the actor network, illustrated by the ad-hoc company strategy. Because of the apparent

lack of enduring elements, the advised actions focused on the development of enduring elements: a corporate slogan, showcase product, market strategy, and a written corporate vision or story. These actions can help a company work towards a well defined and focused market position. The research did not focus on the network dynamics over time, we were unable to provide an estimate of the durability of the advised actions, a prediction of the time for the actions to show effects is also unknown at this point.

### Accountability

DEV2 indicated that nobody was responsible for the security measures within the software (page 88) and results from the interviews indicated a general lack of accountability. We assume that with the communication professional residing at the parent company, accountability for the brand identity is also lacking. If no person feels personal responsibility for the brand identity, the company might fall back to only developing products for the projects they are hired for. This will make the company miss out on opportunities to develop the brand and marking a specific territory on the market. Therefore, for each of the suggested actions, it should be clear who is responsible for the implementation thereof. Furthermore, we suggest to assign someone to the management of corporate values, which also includes evaluating new projects for fit to the corporate values.

### Privacy paradigm

With the found focus on selective sharing within the aspect *use limitation*, the vision on privacy within Sense connects to the idea that privacy is control [19, p. 995]. This idea links to a revised privacy definition stating that privacy is “the ability of individuals to control the terms under which their personal information is acquired and used” [6, p.326]. We observed that privacy is a commodity which can be exchanged for benefits [19, p. 994]. This was mainly expressed in the interview with STAFF2, who described a future for Sense as provider for a marketplace of data. Both these views on privacy can co-exist within the company: people can decide what they share with whom (privacy is control), and may get benefits (privacy as commodity) in exchange for providing their information.

### Communication professionals

As indicated in the part on stable elements, the core concepts of Sense were not clearly defined or documented. The activities of the communication manager of Almende, also responsible for Sense’s communication, mostly involve writing press releases. The apparent complexity of developing a corporate brand might be amongst the reasons this has not been taken up by Sense. We believe that the process described in table 7.3 provides the core concepts present throughout the actor network of the company. This method could therefore help companies with a limited communication department to find the company’s core values.

Step	Action
1	Professional introduces <i>identity types</i>
2	Group places actors in each <i>identity type</i>
2	Group clusters actors within <i>identity types</i> as they seem fit
3	Group describes values associated with company
3	Group clusters values as they seem fit
4	Group links values to actors
5	Group clusters actors with similar values
5	Group discusses and renames actors clusters
6	Professional draws out identity landscapes
7	Professional discusses landscapes with group
8	Group selects preferred set of core values

Table 7.3: Suggested actions performed in a group session resulting in *identity landscapes* representing concepts relevant to the company. This set of actions results in the information transformations shown in fig. 7.3.

#### 7.2.4. Reflection on theory

In this subsection, we reflect on the theories described in section 2.3 and their use in the conceptual model. We describe which new insights into the theories were obtained through our research and also make suggestions to improve on the theory based upon our research. This subsection goes into the theories on brand management, privacy, actor network theory, and brand stability.

##### Brand management

Our research has shown the applicability of the AC<sup>3</sup>ID-model on a small company (< 50 employees), in contrast to the applicability to large and multinational companies (e.g. BP, Volvo, Hilton, and Body Shop) as researched by Balmer and Greyser [2]. In related works the AC<sup>3</sup>ID-model was mainly used to obtain insight in the similarity between the different identity types. However, we extended this by also showing similarity within individual identity types. The visibility of the privacy landscapes also shows a direct overview of inconsistencies within the actor-network, whereas Balmer and Greyser [2] mainly show the connections between identities in figures of the AC<sup>3</sup>ID-model. An apparent gap between company privacy policies and the implementation thereof was indicated by Lahlou et al. [18]. Our results agree with this by showing differences in link to the brand identity between the *personnel* and *product* identities. We furthermore believe that such differences are possible for other concepts besides privacy because products are more rigid elements compared to people [22]. We therefore recommend splitting the actual identity within the the AC<sup>3</sup>ID-model into two identity types representing the personnel and the products separately.

##### Privacy

From the conceptual model, we developed a list of privacy aspects linking end-user concerns about privacy (CFIP [25]), and software design principles on privacy (PFIP [33]). The interview results suggest that these lists do not make up a complete privacy vocabulary. Respondents associated the following unlisted issues with privacy: ownership of the data collected about a person, restriction of access for employees of the company where data is stored, distributed ownership of issues concerning multiple parties, and the depersonalisation of data so that it can not be traced back to an individual. We suggest research is to be done in order to provide an updated operationalisation of privacy. Linking the concerns and implementation on privacy was necessary to enable a common vocabulary throughout the actor network. We believe that stakeholders in the network could benefit from such a common vocabulary because it can directly translate from end-user concern to practical implementation. We recommend the development of a multi-faceted operationalisation on privacy covering end-user concern, practical implementation, and legal terminology.

##### Actor Network Theory

The concepts (punctualisation) and insights (humans and non-humans in one representation) on networks used in this research originated in actor-network theory (ANT). By application of these concepts and insights we were able to create a network containing all entities influencing the corporate brand. These entities were diverse and included products, organizations, gatherings, employees, and legislations. Using the act of punctualisation from actor-network theory we could reduce the complexity of the network from an amount of 75 actors to 10 unique actor clusters. The splitting of the *actual identity* into the two separate identity types *personnel* and *products*, can be viewed as an act of reversed punctualisation because of the apparent conflict within the *actual identity*. The visual approach taken in this research is a novelty compared to the works described in related work [4, 20, 22]. The related works on ANT often elaborately describe situations in large texts. We believe that visual insight in the topology of relations between actors can improve understanding of the reader. We therefore suggest researchers in ANT to apply visual representations more often despite ANT being a rather philosophical approach to actor networks. We did not use ANT to describe the dynamics between actors over time and we could therefore not make any statements regarding the durability of the advice. For practical applicability of the concept, we suggest to look into the dynamic nature of ANT in order to provide stronger advice.

### Brand stability

The model presented by van der Vorst [31] applied link types only to show the link between the brand identity and the products connected, our research applied a derivative of the link types to all entities connected to the brand identity. This application of the concept of link types to multiple identities is an extension to his model. To test it thoroughly, it should be applied to an existing and defined brand identity so that the original link types could be used. We used the frames of reference [31] only in the corporate advice and can therefore draw no generic conclusions on this matter. However, we do find the frames of reference useful for the expansion of core concepts found in products so they also fit the brand identity.

## 7.3. Future work

This section describes the possibilities for future work based upon the research in this thesis. Suggestions for adjustment of used related work will not be discussed in this section and already given in section 7.2.4. Section 7.3.1 suggests further research involving communication professionals to ascertain the practical use of the method for developing *privacy landscapes*. Section 7.3.2 suggests improvements to the measurement of similarity between actors based upon bibliometric mapping of interview responses. Section 7.3.3 suggests to explore different types of visual representation of the actor network, which could also benefit from improved measures for similarity. Section 7.3.4 suggests research into the dynamic nature of networks using network theories and the more general actor network theory. With these suggestions for future work, we have indicated the elements within our research that we think are worth researching.

### 7.3.1. Validation by communication professionals

Positive response on insight provided by the privacy landscapes was attained in personal conversations with Sense's manager on July 3th, 2014. This indicates a possible use for the landscapes in communication advice. However, we did not include any external communication professionals in the research and have therefore only the feedback of Almende's communication manager. We would advise a pilot research to test the usability of the developed method for communication professionals. The requirements of useful tools for communication professionals were not included in this research, and in this way we can examine how the method can best be used by said professionals. Next to this, more research with communication professionals helps validate the general applicability of the developed methodology as discussed in section 7.2.2. We assume a general applicability to other companies, and other or multiple core concepts for the corporate brand. Validation of these assumptions increases the method's strength.

### 7.3.2. Determining similarity measures

This research has focused on the representation of privacy as concept within the corporate brand because of the practical research question asked by Sense. This approach has kept the research focused and manageable. Many companies have a variety of concepts within their corporate brand reported by van der Vorst [31].

To enable application of the developed method to multiple concepts and still obtain an insightful picture, we recommend to develop a similarity measure which determines the similarity between actors. Quantitative similarity measures enable the application of quantitative analyses of the actor network. Translation from qualitative data to a quantitative similarity measure was found in the work of Heersmink et al. [12], who applied bibliometric mapping to show the similarity between terms based upon their mutual occurrence in one source. We suggest to look into the possibilities of applying methods such as bibliometric mapping to cluster responses obtained in structured interviews. This enables to obtain large amounts of results, and clustering these will minimize the observer bias.

### 7.3.3. Improving visual representation

The landscapes portrayed in this research have been limited to one concept per landscape. To enable the visualisation of multiple concepts within the brand identity as discussed in section 7.2.2, the visualisation method should be improved. With multiple core concepts, the original link types used by van der Vorst [31] can be used to display similarity between actors. In general, the links



between actors can become more continuous compared to the current options of *confirmation*, *unknown*, and *contradiction*. Next to a change in link types, a change in visual perspective could help gain better insight into the actors in the network. When talking about how products are influenced, we suggest to place the products in the centre so that the influencing actors and their distance to the products can be seen directly. We recommend to look into different data visualisation options to improve on the given insight into the data.

#### 7.3.4. Identifying effects over time

As discussed in the reflection on actor network theory (ANT), the current approach does not describe the dynamics between actors over time. To gain insight in the durability of the advice, we suggest to develop the method further using more of the dynamic nature of ANT, or apply more quantitative insights obtained in the field of network theory. Estimations on the durability of the advice could be tested by subsequent measurements of the actor network and therewith also validating the methods used from network theory. However, we assume much complexity in this kind of research because of the multitude of influencing factors on the actors within the network. Despite this complexity, we do believe that a better understanding of the dynamic nature of networks can help improve the generated advice.

### 7.4. Bridging fields of study

This section locates possibilities for cooperation between science communication and computer science. We therefore first describe how this research fits into the field of science communication in section 7.4.1. We then continue to look for the addition that computer science can make to science communication in section 7.4.2 and vice versa in section 7.4.3. With this brief review of the possible synergies, we locate opportunities for inter-disciplinary research bridging the two fields of study.

#### 7.4.1. This research as Science Communication

We see this research as science communication because it involves the communication of a company's novel approach to privacy to stakeholders external to that company. The legislation on end-user privacy is still very much under development in the EU [7]. Proper implementation thereof is a novelty in the world of software development because it is not often a design requirement [19]. With the exploratory research in this thesis, we found a way to translate beliefs on end-user privacy into a core concept within Sense's corporate brand. This translation enables the company to better communicate their beliefs on privacy. The developed *privacy landscapes* can possibly serve as a decision support tool for companies looking for a method to translate 'soft'-values and beliefs into core concepts within their corporate brand.

Because of the application of brand management theories, the research in this thesis can also be seen as marketing research. Due to the research being carried out as part of a thesis to acquire a masters degree in science communication, we approach this research as science communication research.

#### 7.4.2. Computer science's addition to science communication

The future work described in section 7.3 shows possibilities of applying theories from computer science into this work on science communication. The final two recommendations on future work include suggestions for application of data visualisation techniques and network theory.

The visual representation developed in this thesis shows how data visualisation can help communication professionals gain insight in the complex network of actors that influence the corporate brand. We believe that proper data visualisation can improve decision making processes by providing a comprehensive overview of the situation at hand. In general, theories on data visualisation may help the field of science communication by providing new insights in the workings of visual communication.

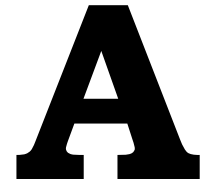
The fields of network theory and also systems theory have already made a brief appearance within this thesis: van der Vorst [31] took a systems theoretical approach to branding, and our implementation of actor network theory makes it possible to develop this method using network theory. The suggested future work on effects over time can benefit much from network theory and

the dynamics described in actor network theory. The developed method can produce more certain advice with applied knowledge on the effects of changes to the network topology, or motivation of single actors to steer the network. For example, application of systems theories to science communication can help to gain insight for stakeholder analyses in a connected world.

When actors within such a network are properly described in terms of values and interactions, agent based modelling can be used to simulate the effects of adjustments to actors or their network. In this way, it could be possible to test what the effect of applying a specific means of communication could have on the targeted audience.

#### **7.4.3. Science communication's addition to computer science**

The results of this research show how core values of a software company are represented in the products. Applying the developed methodology can make a company aware of the relation between products and the corporate brand. Taking the corporate values into account when designing software and choosing clients, can enforce the corporate brand through confirmation of and exposure to these values. Researching the corporate values in relation to developed software, can help bring meaningful and value-based software design. Theoretical models on motivation and framing as found in science communication, can help to develop more effective software for personalized healthcare. An example of such a program is a personalized lifestyle coach advising based upon what motivates you, or can learn your motivations by tracking effectiveness of suggestions. In the same line of thought, agent based modelling and simulation of human processes can also benefit from a better fitting description of human motivation and behaviour so as to improve the models of human actors. In the field of situational awareness, multi agent systems consisting of both humans and robots working on a collective goal could benefit from science communication in the development of shared mental models. Theories on learning, motivation, and communication can help the system to enable useful information exchange between agents.



## Results per search query

search clusters	Scopus	
	TAK	ALL
B	4518	
P	40284	
N	29498	
T	65561	
S	12884	
<hr/>		
$B \cap P$	16	
$B \cap N$	26	
$B \cap T$	204	
$B \cap S$	17	
$P \cap N$	0	
$P \cap T$	3	
$P \cap S$	0	
$N \cap T$	165	
$N \cap S$	17	
$T \cap S$	401	
<hr/>		
$B \cap P \cap N$	0	2
$B \cap P \cap T$	6	56
$B \cap P \cap S$	0	2
$B \cap N \cap T$	0	34
$B \cap N \cap S$	0	0
$B \cap T \cap S$	0	3
$P \cap N \cap T$	0	334
$P \cap N \cap S$	0	92
$P \cap T \cap S$	116	1410
$N \cap T \cap S$	0	46
<hr/>		
$P \cap N \cap T \cap S$	0	27
$B \cap N \cap T \cap S$	0	0
$B \cap P \cap T \cap S$	0	2
$B \cap P \cap N \cap S$	0	0
$B \cap P \cap N \cap T$	0	2
$B \cap P \cap N \cap T \cap S$	0	0

Table A.1: Amount of results on queries which combine the search clusters branding (B), privacy (P), trust (T), software (S), and network (N)

# B

## Questionnaire

The questionnaire in this chapter is the one used to structure the semi-structured interviews. It is used as a handhold during the interviews and therefore the questions are not guaranteed to have been asked in this order. The questions are all in the original language (Dutch) and answers to these questions are found in appendix C.

### Netwerk

Met wie of wat uit deze partijen heb je te maken en in welke vorm? Teken deze uit in een netwerk beginnend vanuit jezelf, van nu naar toekomst

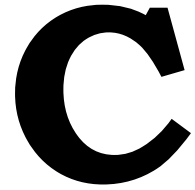
- Actual identity
  - medewerkers
  - producten
- Communicated Identity (expliciet dingen als website (middelen) vermelden)
  - communicatiemedewerkers
  - media en pers
  - (externe) evenementen
- Conceived identity
  - externe partijen
  - partners
  - klanten
  - eindgebruikers
- Ideal identity
  - concurrenten
  - beleidsmakers (in het bedrijf)
  - wetgevers
- Desired identity
  - (top) management

## Privacy in het netwerk

- Wat is privacy volgens jou?
  - Principles of Fair Information Practice [19]
    - ◊ openness and transparency
    - ◊ collection limitation
    - ◊ individual participation
    - ◊ data quality
    - ◊ use limitation
    - ◊ accountability
    - ◊ reasonable security
  - Concern For Information Privacy Smith et al. [25]
    - ◊ secondary use
    - ◊ errors
    - ◊ collection
    - ◊ unauthorized access
- Hoe denk je dat de andere partijen in je netwerk over privacy denken?

## Merkbelofte

- Merkbefofte
  - Als Sense een belofte over privacy zou maken, wat zou hier dan in moeten staan?
- Clusteren
  - Zou je partijen in je netwerk kunnen clusteren op basis van privacy-denken?
  - Hoe verschillen de clusters die je zojuist gemaakt hebt?
- Effect van merkbefofte
  - Wat moet er gebeuren om de belofte die jij voorstelt waar te maken?



## Interview transcriptions

This chapter gives the ad verbatim transcriptions of the interviews held with employees of Sense and the parent company Almende and are used in chapter 4 to create the network representation for the company as well as fill in the beliefs on privacy throughout the network. The transcriptions are in the Dutch language and have been created using the video recordings of the interviews. The interviewers text is preceded by 'I:,' whereas the respondents text is preceded by 'R:.' Wherever text was unrecognizable, this will be denoted by three dots: '...' Special events during the interviews (e.g. long pauses) are denoted between brackets: '[event description]'. Section headers are added for easy reference and represent the subject at that particular stage of the interview. For anonymity, the respondents have been named Developer (DEV) 1 to 4, and Staff (STAFF) 1 to 4. Because having developed a sense of "who we are as a company" was a selection criterium in line with Gioia et al. [10], the new employee DEV5 was not selected as a respondent for the interviews. DEV5 was mentioned by some respondents. Staff member four (Staff 4) has participated as test-interviewee and was not recorded on video. Therefore, a thorough transcription of that specific interview is missing, and has been replaced by a summary which was validated by the respondent.

### C.1. Developer 1

[936\_0298].mov

R: geen overheadmicrofoon?

I: nee ik heb gisteren geprobeerd maar die nam niet zo lekker op. Deze pakt zeg maar wel de hele ruimte en wat die overhead microfoon wel doet die heeft waarschijnlijk 3 meter bereik ofzo en daarna valt het weg. Iets wat op zich met een drumstel wel handig is maar verder niet echt. Wat we gaan doen is we gaan kijken van uit jou met ie je allemaal te maken hebt vanuit Sense zeg maar, met welke tijen welke documenten, objecten, software, en dan gaan we aan de hand van dat netwerk en aan de hand van jouw visie op privacy kijken of daar in dat netwerk ergens tegenstrijdige visies zitten en wat daar allemaal mee te doen is qua privacy. Is dat tot zover duidelijk?

R: Nee niet helemaal maar

I: niet helemaal

R: ik denk dat ik het wel zie

I: okay, Wil jij op het whiteboard tekenen of zeg jij ik wil wel op een papiertje tekenen

R: ik wil wel op het whiteboard tekenen.

I: dat is mooi

R: dat vind ik wel leuk

### Network

I: Dan mag je op het wb tekenen in het midden een poppetje wat je zelf voorsteld. Dan wil ik wel weten met welke, noem een een top drie van mensen binnen Sense waar jij mee te maken hebt

R: De top drie waar ik mee te maken heb. En nu hier om heen trekken?

I: Even kijken, die mogen in deze hoek een beetje

R: okay. Dat is STAFF3 dat is ook wel DEV3 denk ik

I: Als je er niet helemaal uit komt met drie dan mag het er ook wel een meer of een minder zijn hoor

R: Ik denk dat het DEV3 en DEV4 zijn. Maar Ik weet niet precies hoe jij het zou willen meten, maar.

I: okay En welke producten van sense heb jij vooral mee te maken. En die mogen hier ergens (bord) En wat voor logootje je daarvoor wilt verzinnen mag je helemaal zelf weten.

R: Welke produkten van Sense?

I: Ja welke produkten of zeg maar software, Dingen die ontwikkeld worden door Sense. Zal ik ondertussen even het raam open zetten?

[2:50]

R: nou dat is MiriaNed, dat is commonsense platform/API

I: Telt dat commonsense telt dat als frontend of backend

R: Als backend gebruikt

I: okay

R: En ja alles wat ik zelf ontwikkel voor greenhouses.

I: Ja. En dat is?

R: Greenhouses: Alles wat greenhouse is. Dat is de koppeling met klimaat computers de mapping van dingen van klimaatsensoren en klimaatcomputers naar commonsense, die hele modulatie, beetje front-end dingetjes daarvan

I: En zeg maar van de mensen die hier staan en de toepassingen of artikelen zeg maar produkten die daar staan heb je daar ook samenwerking mee dat je zegt van nou de commonsense en API daar hebben andere mensen ook mee te maken? Kan me voorstellen dat DEV4 er ook mee te maken heeft.

[4:42]

R: Ja compatibility is wel een hele duidelijke link.

I: ja

R: En STAFF3 heeft het vooral met greenhouse, ja eigenlijk met alles wel maar ja vooral met greenhouses

I: Zou je daar een lijntje tussen kunnen zetten tussen STAFF3 en wat hij dan doet en ook DEV4 en DEV3

R: Ja DEV3 heeft hier eigenlijk niet zo heel veel mee te maken

I: Waar heb jij het zeg maar qua, waar heb jij het dan met DEV3 vaak over. Jij zegt belangrijke belangrijke mensen met Sense daar heb je geen produktontwikkeling mee samen.

[5:20]

R: Nee, eigenlijk niet volgens mij

I: Dat geeft niet. Qua externe communicatie van Sense zeg maar mensen die de boodschap van Sense of Sense dit is wat we doen naar buiten brengen, wat voor mensen heb je daar voor mee te maken.

R: Binnen Sense of buiten Sense

I: Mag allebei Dat mag ook de pers zijn vaklui

R: Zijn dat mensen die vertellen over Sense aan de buitenwereld of mensen aan wie ik over Sense vertel ofzo

I: Mag allebei Zeg maar Alles wat er voor zorgt dat dat Sense uiteindelijk naar de buitenwereld over gecommuniceerd wordt Dat mogen bijvoorbeeld interne communicatie mensen zijn

R: Waar wil je die hier hebben

I: doe maar links hier

R: Dat is bijv. Martin bij Green Formula en dat is Lex bij Devlab en dat is andere mensen van DevLab en mensen van de hogeschool toch ook wel

I: Je mag wel hogeschool neerzetten hoor dat is prima

I: Heb je ook beurzen of workshops waar je van zegt daar doe ik regelmatig aan mee? dingen waar je dan bijv de dag van de zelforganisatie.van zulk soort demos presentaties

[7:30]

R: Ja DevLab-dag

I: Ja

R: Ik kan DevLab er als geheel er wel bijzetten, wat is het logo daarvan?



I: Volgens mij driehoekje iets

R: Ja misschien nog de mensen in het Simple-project. Daar hebben we ook nog wel aan het Sense. Dat zijn niet echt mensen bij die zelf weer Sense promoten.

I: Dus dat houdt daar op.

R: ja

I: En publicaties wordt er gepubliceerd over Sense

R: ja ik weet het zeker dat ik met STAFF4 een keer iets heb gepubliceerd, en verder soms nieuwsberichten ofzo

I: maar daar ben je zelf weinig mee betrokken

R: Over onze activiteiten in de kassen zijn diverse nieuwsberichten geweest

I: Waar komen die terecht die nieuwsberichten?

R: In van die automatiseringsbladen en websites enzo

I: okay maar die worden dan geschreven door?

R: Door STAFF4. zal ik die er bij zetten

I: Ja dat mag want ik neem aan tenminste ik neem aan dat als STAFF4 dan contact met jou op neemt hoe werkt dat dan precies

R: ja dat wel

I: Ja dan mag STAFF4 erbij. Dan gaan we nu naar de rechterkant. En daar wil ik wel hebben externe partijen zoals klanten partners en eindgebruikers waar jij mee te maken hebt dat mogen partijen zijn waar jij mee samen ontwikkeld.

R: [schrijft bedrijven op] Ja je hebt ook weer mensen in het Simple project maar dat is niet echt Sense specifiek

[10:32]

I: Dat is meer de sensor netwerken. Het is natuurlijk het sensornetwerk is wel onderdeel van Sense toch

R: ja maar in Simple zitten we als Almende. Maar dit zijn echt wel allemaal (eind)gebruikers van Sense. Als dat van Almende is waar zou je Almende plaatsen?

R: poeh

I: paar clubjes. ou dat tellen als een partner bedrijf in brede zin

R: ja misschien wel maar goh dat vind ik moeilijk want dit waren dit zeg waar mee ontwikkeld die soort van gebruikers zijn van Sense toch

I: Eh nou ja van Sense als platform nou ja meer waarmee je ontwikkelt als bedrijf zijnde

R: Ja in die zin natuurlijk wel omdat ik zeg maar aan de ene kant voor Almende werk en de andere kant voor Sense dus in die zin werk ik met mezelf samen

I: ja oke

R: en zou je Almende daartussen kunnen plaatsen

I: Maar jij zegt hij past daar misschien niet helemaal bij

R: Ik schrijf het er gewoon bij. Het is een beetje ja ik weet niet

I: Het is meer dat dat binnen jou zelf eigenlijk een stukje Sense en Almende zit

[13:00]

R: mijn Sense gedeelte zeg maar heeft niet heel veel van doen met Almende meer alhoewel daar nu wel ook een sensor netwerk draait voor localisatie bijvoorbeeld. dat zou je dan wel kunnen zien als een soort partnership

I: als dat jouw sensor netwerk is dan ja. Even kijken deze hier neerzetten zou jij hier rechtsonder voor mij kunnen neerzetten wie eigenlijk de belangrijke concurrenten zijn van zijn Sense. Als jij zegt daar heb ik helemaal geen verstand van dan mag dat ook

R: Een concurrent is Let's grow dat gaat puur over de tuinbouw wereld maar daar doen zij een soort van hetzelfde online platform waar alle data naar toe kan alleen is dit echt moeilijk te noemen geavanceerd maar dat is in die zin wel een concurrent kunnen moemen

I: En bieden zij ook de hardware daarbij

R: Nee maar wij ook niet

I: nee okay

R: Dat gaat daar zijn wij zijn nu bezig dat Chess dat gaat doen

I: ja

R: wat zij vooral niet bij bieden is Green Formula

I: ja

R: en gestandariseerde weergave van de data. Wat zij brengen is gewoon zeg maar van sensor-naam en data hup export en dan basisbestand de datum zie maar wat je er mee doet. wij proberen ook nog te standarisieren zodat het voor alle kassen kunt vergelijken zeg maar. Verder zijn er ook wel een heleboel kleine concurrentjes denk ik maar die allemaal een gedeelte doen wat wij ook doen zeg maar daar kan ik niet zo heel goed opkomen eigelijks

[15:00]

I: Zijn er mensen of bedrijven die eigenlijk precies hetzelfde doen als Sense?

R: Nee

I: Waarin is Sense dan bijzonder?

R: In de interpretatie van data. Wij doen alles wat we om data opslag heen hebben ingebouwd.

I: Algorithmes?

R: Ja, algorithmes, maar ook de triggers en het delen ervan. Het feit dat je wat voor data dan ook erin kwijt kan, dat daaraan geen restricties verbonden zijn. Het is een heel generiek platform. Het stelt mensen in staat om op wat voor manier dan ook te gebruiken. Er zit wat dat betreft niet echt een limiet aan. Ik denk dat dat wel heel sterk is. Met MiriaNed doen we een beetje hetzelfde, er is heel lang naar gezocht en de basis is nu een beetje hetzelfde. Een nieuwe student neemt die basis voor waar aan en gaan meteen aan de slag die zien bijvoorbeeld dat als ze ergens geen bereik hebben "o wacht eens even, ik zet er gewoon extra nodes ertussen en dan werkt het weer." Mensen gaan zelf op zoek naar oplossingen en kunnen zelf bedenken 'dit past op die manier in de database' en 'dit kan ik op deze manier oplossen'

I: Omdat je het zo generiek hebt gemaakt dat iedereen er wel wat mee kan doen?

R: Ja, en ik denk bijvoorbeeld bij Cosm dat het heel rigide is. Wat er kan is er sensordata in uploaden, eens per vijf minuten en op die kaart kun je dan klikken en krijg je een grafiekje en dat moet dan een float zijn anders krijg je er geen grafiekje van

I: Ah ok. Dan een vraagje over het beleid van het bedrijf. Wie hebben daar het meest mee te maken? Met waar gaan we heen als Sense zijnde?

R: Waar wil je die hebben?

I: Hier ergens. [wijst op whiteboard]

R: Hier binnen Sense?

I: Je mag ook opschrijven dat als het beleid van Sense veelal wordt bepaald door mensen buiten Sense, dan mogen die er ook zeker bij.

R: Ik zet STAFF2 een beetje aan de zijlijn erbij. En verder denk ik gewoon DEV3, DEV4, DEV1 en STAFF3.

I: Ok.

R: Misschien ook wel gewoon het landschap waarin we opereren.

I: Dat bepaalt waar je mogelijkheden zitten?

R: Precies.

I: Vandaar ook dat ik zei dat je de concurrenten erbij kan zetten om te kijken waar Sense tussen zit. Wat voor elementen in dat landschap bepalen dan vooral waar Sense heen kan?

R: Vooral waar de grootste kansen liggen. Het bepaalt niet zozeer waar het heen kan, maar waar het heen gaat. Ik zie het een beetje als 'we gaan gewoon die kant op', waar het snelste binnen te halen is.

I: Waar is dat op dit moment?

R: In de zorg, heel erg.

I: Zou je die daar ook bij kunnen zetten?

R: Waar?

I: Hier. [wijst op whiteboard] Want die bepaalt dan wel jouw beleid. Als je zegt de zorgsector is hetgene waar we naar toe gaan, dan zullen de wensen vanuit de zorgsector bepalend zijn voor wat je doet als bedrijf.

R: Wat dat betreft ook de glastuinbouw. En DevLab misschien ook wel. Dat is ook een partij waar we veel mee te maken hebben.

I: En als daar projecten binnen zijn stuurt dat natuurlijk ook weer waar je naartoe gaat als bedrijf.

R: Maar goed, dat is misschien een beetje een DEV1-centrisch beeld van waar we naartoe gaan.

I: Het is met iedereen binnen Sense en dat geeft een totaal beeld. Wie zou er volgens jou het meest bepalend zijn voor de visie van Sense?

R: Ik denk deze mensen, misschien dat daarvan STAFF2 nog wel wat hoger staat. Die is vooral in

de opstartfase bepalend geweest, inmiddels wat minder, iedereen zegt nu we zijn nu zelfbepalend. Ik weet niet goed wat de invloed van STAFF2 op STAFF3 is.

I: Nee, dat moet ik dan weer aan STAFF3 vragen.

R: Ja.

I: Ok. Dat is het stukje netwerk tekenen.

[21:50]

## Privacy

I: Wat is privacy volgens jou?

R: Zo, tering.

I: Deze vraag moet dus duidelijker ingeleid worden.

R: Misschien eerder aankondigen? Wat is privacy...

I: Met name in relatie tot Sense.

R: In het algemeen is het het idee dat je recht hebt op het geheim houden van dingen die jou aangaan. En ja in relatie tot Sense is dat nog steeds hetzelfde ongeveer, maar gaat het dan over data die over jou verzameld is.

I: En wat zou er met die data moeten kunnen of moeten gebeuren om te zeggen dat het goed rekening houdt met de privacy wensen van degene van wie de data is.

R: Als privacy gedefinieerd is als geheimhouding van de data, dan moet je zelf kunnen beslissen aan wie je data publiceert, aan wie dan ook.

I: Zou dat dan ook zover gaan als dat je dat bijvoorbeeld, als ik bij Sense mijn data opsla, dat ik en echt alleen maar ik bij de data hoort te kunnen?

R: Ja.

I: Dus ook niet mensen van Sense?

R: Ja. Het moet zeker zijn. Het wil overigens niet zeggen dat ik het idee van privacy onderschrijf.

I: Nee. Hoe bedoel je dat?

R: Ik denk dat het idee van privacy vooral geboren is uit schaamte. Niet iedereen mag weten wat ik doe. Je wil alleen maar dingen als het op een of andere manier schadelijk voor je is. Dat is omdat het anders is dan wat de rest doet of je verwacht dat het anders is dan wat de rest doet.

I: Dus als je een of andere rare hobby hebt en je wilt niet dat andere mensen dat zien?

R: Ja, en vanuit het idee dat iedereen wel een skelet in de kast heeft is het, dan is vooral denk ik een kwestie van acceptatie en tolerantie. Ik denk ook dat veel mensen heel panisch zijn over privacy. Er zijn een heleboel dingen die meer dan een mens aangaat, waarbij het hele idee over privacy, dat iedereen zijn privacy zo strak handhaaft als zou moeten kunnen, dan is het onmogelijk. Aan de ene kant is het mijn privacy dat niemand weet waar ik gelopen heb, maar iedereen kan mij zien als ik daar loop. In die zin heb ik al veel privacy opgegeven. En ja, dan is dus het idee van mijn data dat ik daar gelopen heb niet met vreemden gedeeld mag worden misplaatst, want dat is al gebeurd.

I: Iedereen die je daar bij het kruispunt hebben zien lopen die ken jij in principe niet.

R: Maar die hebben al de data dat ik daar gelopen heb. Met dat idee wordt privacy enorm overschat, omdat een heleboel data voor het gros van de mensen niet interessant is en je dus privacy op moet geven om de data te delen.

I: Maar als die data niet voor hun interessant is, waarom zou je die dan wel gaan delen? Wat voor voordeel kunnen ze hebben?

R: Je hoeft het niet expliciet met hen te delen. Je geeft geen privacy op als je expliciet je data beschermt van al die mensen. Maar het heeft voor jou geen negatieve invloed als ze beschikking hebben over de data.

I: Ja. Hoe zit dat met het verzamelen van allemaal van dat soort data? Stel je zou van alle lopende mensen door heel Rotterdam data verzamelen. Is dat een issue of worden mensen daar ongelukkig van? Word jij daar ongelukkig van?

R: Nee, ik niet. Sommige mensen wel. Sommigen jengelen over 'big brother' en complottheorieën. Toe maar, hoor. Zodra je dat soort dingen voor 'evil' gaat gebruiken. Dat heeft ook niet zoveel met privacy te maken eigenlijk.

I: Ok. Denk jij dat er zegmaar van de partijen die op het bord staan, dat die allemaal hetzelfde denken over privacy dan dat jij er over denkt?

R: Nee.

I: Wie denken er het meest radicaal anders? En wat denken die dan?

R: Nou, ik denk dat er een heleboel mensen wel heel veel waarde hechten aan privacy. En ja, wie dat precies zijn. Ik denk dat er sowieso buiten Sense veel mensen zijn. Ik vind dat moeilijk om dat allemaal in een schaal te plaatsen. Ik bedoel, privacy is een heel hot issue. Het geeft aan dat heel veel mensen het belangrijk vinden en gehecht zijn aan het idee van privacy. Dus ik denk dat ik daar een radicaal ander beeld over heb.

I: Jij zegt, privacy bestaat eigenlijk niet.

R: Het is iets ingewikkeld, het wordt ontzettend overdreven. Sommige mensen vinden dat het niet goed is dat je altijd een ID-bewijs bij je moet hebben vanwege het recht op privacy. Je bent wie je bent, ook als je geen ID-bewijs bij je hebt en als een politieagent je vraagt wie je bent en je laat dat zien...

I: Ben je sneller klaar.

R: Hoeveel informatie heb je nou in wezen over jezelf opgegeven? Eigenlijk geen zak. Ik denk wel dat er een redelijk verband is tussen leeftijden in het omgaan met privacy.

I: Hoe bedoel je?

R: Ik denk dat met name sociale media en dingen als facebook enzo er wel voor zorgen dat jongere mensen minder strak met privacy omgaan dan oudere mensen. Het is best wel persoonlijke informatie die gedeeld wordt op facebook. Eigenlijk doen mensen vrijwillig al veel meer afstand van privacy.

I: Waarom zou dat zijn? Krijgen ze er dingen voor terug.

R: Nee, het is gewoon de norm denk ik.

I: Het is de sociale druk?

R: Nee, het is niet de sociale druk. Het is technologie die het mogelijk maakt om heel veel data en heel veel informatie over jezelf te delen en het moeilijk maakt om niet heel veel informatie over jezelf te delen. Ik weet niet of het echt sociale druk is, maar ik denk dat dat een soort nieuw model is die zich ontwikkelt. Je kan zeggen 'je kan niet op facebook en dan val je buiten je sociale groep' en in die zin is het sociale druk. Het is voor de meeste jonge mensen niet een 'trade-off', het is niet dat iedereen denkt 'we moeten op facebook, want privacy!', het is meer 'we moeten gewoon op facebook.

I: Dus eigenlijk maken jongeren zich minder druk om privacy?

R: Veel minder, natuurlijk, want er wordt nog steeds niet alles gedeeld.

[33:00]

I: En nog even terug naar bedrijven en projecten waar jij mee bezig bent. Bijvoorbeeld die kassen. Is daar sprake van dingen waar privacy een rol kan spelen? Dan gaat het natuurlijk over de privacy van de bedrijfsdata, bijvoorbeeld.

R: Ik vind het daar ook weer een roddel dat je aan de ene kant dat ze het aan de ene kant heel goed vinden om data van elkaar te delen en van elkaar te leren. Alle telers zeggen 'we zijn geen concurrenten meer, want als wij gaan concurreren dan zijn we in een keer van de markt, dus we moeten samenwerken om de technologische voorsprong die we hebben te behouden.' En daarvoor gaan ze dus ook bij elkaar kijken en praten 'hoe doe jij dingen?' wat dat betreft hebben ze qua bedrijfsvoering al heel weinig privacy meer. Aan de andere kant, als het gaat om data in de cloud, dan wordt wel meteen gedacht 'dan moet het secure', 'dan is privacy belangrijk'. Dan moet er gelijk een kluisje om, zodat niemand anders erbij kan.

I: En dan alleen de mensen die zij vinden dat erbij mogen?

R: Ja.

I: Zijn dat dan wel de bedrijven waar ze normaliter mee samenwerken?

R: Jaja. Dat het platform het mogelijk maakt de data te delen vinden ze dan wel weer leuk. Dat is een pluspunt van het platform.

I: Ze willen dan niet dat een willekeurige groenteboer ergens kan gaan kijken?

R: Daar hebben ze het niet eens over. Dat lijkt me ook niet. Een ander ding, veel van de telers telen biologisch, dat moet wel op die verpakkingen en als iedereen zomaar in die kassen kan kijken en kan zien wat er gebeurt dan is dat natuurlijk ook een bewijs dat je biologisch teelt. Dus, ik weet niet, het is een beetje een mindset dat als je het woord 'privacy' opzet, je meteen 'waah, moet beschermd.' We kunnen er voor zorgen dat het niet op straat ligt en dat is natuurlijk ook zo, maar aan de andere kant doen ze het zelf wel.

I: Maar ze willen zelf bepalen welke straat?

R: Nee, dat ook niet echt. Nee, daar hebben ze ook niet genoeg verstand van.

I: Maar ze zijn in de basis dat ze denken dat ze zelf de data willen hebben en het mag niet zomaar naar iedereen toe. Alsin ze hebben daarin verschil met jou.

R: Ze hebben niet een eenduidig standpunt. Ze zijn wel van openheid en data delen en inzicht geven, maar aan de andere kant hebben ze wel een panische paniecreactie wanneer je zegt dat het de cloud in gaat. Dat is niet echt rationeel geloof ik. Beetje zoals ze zeggen "je kunt iets niet twee keer invriezen!"

[36:30]

I: Echt wel.

R: Ja, precies, maar het is zo'n, heel veel mensen springen op, alle stoppen gaan los en er wordt niet meer rationeel gedacht. Zo werkt dat ook met privacy. Zodra je begint over data delen beginnen mensen te roepen 'privacy dit, privacy dat' en ja, weet je wel, stop zit en relax, denk er even over na en dan is het allemaal niet zo erg.

I: Hoe denken ze er eigenlijk bij Amende over? Omdat Amende nogal dicht bij de gebruikers staat.

R: Dat wee tik eigenlijk niet, moet je aan STAFF2 vragen. Judith lijkt me iemand die daar echt heel erg bovenop zit, maar het verschilt sterk per persoon denk ik.

I: Misschien de mensen bij Worm? Hoe denken die daarover? Dat is misschien nog maar heel kort dat je daarmee samenwerkt.

R: Ik denk dat die daar veel losser naar kijken. Die willen ook graag een beetje provoceren en laten zien wat kan met je techniek en als iets kan met bepaalde technieken met smart phones en met sociale media is privacy .... En waar ik het ook met ze over gehad hebben is dat ze mensen vertellen bij binnenkomst dat je weet dat je gecheckt kan worden en 'weet dat je hier een stuk van je privacy inlevert als je hier binnenkomt.' Nouja, dat is een manier waarop mensen aan het denken gezet worden en een manier waarop je kan confronteren dat je eigenlijk heel vaak gewoon openbaar bent. Ik denk dat zij er ook veel opener in zijn.

I: En...[kijkt naar bord]

R: Binnen Devlab in het algemeen is het heel hot.

I: Want, hoe zit het binnen devlab?

R: Ja, daar kan dus heel veel meer. De security met merineb maakt dat mogelijk. Bijvoorbeeld de hartslag van ouderen wordt over internet verstuurd en ik vraag me nog steeds af waarom dat niet zou kunnen. De kans dat iemand 'meeluisterd' is bijzonder klein en als hij meeluisterd, ja dan weet hij de hartslag en dan... Als je iemand om wilt leggen loop je gewoon het verzorgingshuis binnen met een pistool en dat ga je dan niet via merineb doen. Wat heeft iemand er nou aan wat de hartslag van een oudere is.

I: Als het bijzonder een verzekeraar is die op basis van die data net eventjes andere aanbiedingen kan doen van zorgverzekering.

R: Je kan altijd Big Brother verhalen erover bedenken. Ja, dat is een reëel gevaar wat je ook altijd hebt.

I: Waar je op andere manieren weer afspraken over kan maken? Dat je op basis van deze gegevens niet de prijzen aan mag passen.

R: Daar bestaan al wetten over dat dat niet mag. Dat is ook het hele idee van een verzekeringssysteem. Iedereen betaalt een klein beetje voor de grote uitgaven van een ander.

I: Dat is zo.

R: Dus ja, op zekere hoogte kan ik begrijpen dat dat je sommige data niet aan een verzekeraar wilt laten zien. Hoewel je als je heel gezond bent je dat misschien weer wel wilt als je in aanmerking komt voor een lagere premie. Maar die fout zit vooral in het systeem van verzekeraars dan, niet zozeer bij het opgeven van privacy. Het feit dat je 86 bent en in een verzorgingshuis zit maakt dat je meer likely bent om grote uitgaven te doen.

I: Maar denk jij dat er in de zorgsector ze het meest geven om privacy van alle clubjes die op het bord staan?

R: Ja, ik denk het wel.

I: Zouden ze daar veel waarde hechten aan als je zou zeggen "wij van Sense zorgen dat je zelf over je data qua privacy kan beschikken."

R: Dat zou een eerste vereiste zijn.

## Covenant

I: Gaan we verder naar het volgende puntje. Stel je voor jij zou Sense zijn of jij zou bepalen hoe Sense naar de wereld zich zou moeten uiten. Wat zou jij dan, als Sense zijnde, de wereld willen beloven met betrekking tot privacy?

R: Ik vind opzich de belofte dat jij de enige bent die over de data kan beschikken en dat jij de gene bent die bepaalt met wie je het deelt, vind ik een goede belofte. Aan de ene kant is privacy erg hot, maar aan de andere kant is het gewoon de dienst die we verlenen waarbij we de mensen de mogelijkheid bieden om data over zichzelf te verzamelen. Het is logisch dat het jouw data is en niet die van een ander en dat jij daar zeggenschap daarover hebt, maar meer alsin dat jij een fiets koopt en dat jij daar zeggenschap over hebt, dan in de zin van dat het persoonlijke data is dat ten allen tijden beschermd moet blijven worden.

I: Het is meer dat het "jouw stukje dienst is" en dat jij daar zeggenschap over hebt?

R: Ja, het is jouw product.

I: Denk jij dat eigenlijk de rest van de mensen of partijen die op het bord staan dat die er ook van bewust zijn dat dat de dienst is die Sense biedt?

R: Ja, van ons wel.

I: Misschien niet de concurrenten?

R: Ja, ik zeg er altijd bij dat het op die manier werkt. Ik breng het altijd wel als zijnde privacy.

I: Zijn er ook mensen die zeggen dat het heel vernieuwend of anders is dan wat ze hadden verwacht?

R: Als ik over Sense begin te vertellen? Iedereen.

I: Maar ook met betrekking tot de data is van jou en jij bent de enige die daar beschikking over heeft.

R: Nee, dat wordt meestal als normaal ervaren. De eerste reactie is "wat ontzettend gaaf" en de tweede "Maar ja, privacy" en als je dat vertelt, dan is het vaak "Ja, dan kan het wel."

I: Denk jij dat al die partijen op het bord, in hun product, zelf ook passen bij het standpunt van de data is van jou en je mag zelf bepalen wat je ermee doet? In hun producten of diensten of wat ze ook maar doen.

R: Ja, want volgensmij de meesten van hen is wat ze doen oplossingen voor klanten bouwen. [Mompelt enkele meimeringen] Bij Let's Grow is het misschien wat meer dat als je het wilt uploaden dat je moet kiezen of je het wilt delen of niet.

I: Ok.

R: Zegmaar, bij bij PatchBay is het vaak zo dat anderen pas géén toegang krijgen tot je data als je er voor betaalt.

I: Dus het is standaard openbaar, maar als je betaalt hebt...

R: Volgensmij was het bij PatchBay zo dat je een kaartje kreeg met allemaal sensoren erop en dan kon je op die sensor klikken en kreeg je een grafiekje. Als je niet wilde dat jouw data daarop kwam, moest je betalen.

I: Ja.

R: Maar dat weet ik niet meer precies.

I: Telt PatchBay ook als een concurrent?

R: Dat is Cosm inmiddels. GreenFormula hanteert dat wel; applicaties zijn echt van jou. Chess ook. Het is bij hun vaak zo met loginkastjes enzo. Ja, Worm zal dat wat minder doen.

I: En waar het laatst over ging, dat in de zorg patient en behandelaar allebei data in willen zien. Hoe valt dat samen met de data is van jou? Van wie is die data?

R: Van de patient. Van de persoon over wie het gaat.

I: De patient zegt dan ik deel het met mijn dokter?

R: Ja.

I: Dat bericht, of de belofte, data is van jou en jij bent de enige die bepaalt wat er mee gedaan wordt. Dat is eigenlijk wat er nu al uitgedragen wordt en wat voor iedereen die voor het eerst in aanraking komt met Sense al duidelijk is? Of mist daar nog iets?

R: Ik weet niet of het meteen duidelijk is als je download uit de appstore of market. Het is overigens wel wat we uitdragen, maar nog niet echt goed geïmplementeerd, want wij van Sense hebben wel toegang tot alle data.

I: Ja.

R: En dat is eigenlijk illegaal.

[50:00]

I: Is daar wat aan te doen? Kan dat anders?

R: Volgens mij was het idee om alle data te encrypten die de database in moeten, maar dat brengt een heleboel performance-issues met zich mee.

I: Maar dan zit er dus eigenlijk in het stukje rechts boven, het stukje software en producten, niet ingebouwd?

R: In common sense. Dat is wel het enige waar het niet geïmplementeerd is. Ik weet niet hoeveel mensen toegang tot de database hebben, dat zullen maar een man of drie of vier zijn, dus wat dat betreft doen we het best aardig.

I: Hoe weten we zo zeker dat die mensen te vertrouwen zijn?

R: Dat weten we niet.

I: Dat weten we niet, maar...

R: Vertrouwen? Ik vind dat ook weer zoiets, waarom zou je ze moeten vertrouwen? Ik bedoel wat kun je met die data? Ik zou niet eens willen weten waar al die mensen uithangen, het interesseert me geen zak. Het is informatie waar ik geen kont mee kan. Moeten we ze kunnen vertrouwen? Misschien wel, misschien niet. Misschien moeten we ze vertrouwen dat ze het niet aan anderen doorverkopen.

I: Ja, maar daar heb je nergens voor getekend? Dat jij met wat je hier doet voor werk dat je die data niet doorverkoopt. Tekenen is natuurlijk ook maar...

R: Dat weet ik niet, daarvoor zou ik mijn contract even na moeten lezen. Ik weet niet of data die door Sense voor klanten wordt verzameld ergens onder valt.

I: Het is waarschijnlijk wel dat producten die je maakt voor Sense dat je daar zelf niet meer wat mee mag doen. Ok, dus qua de data is van jou is op dit moment in dit netwerk alleen Common-Sense afwijkend.

R: Ironisch he? Ja, misschien dus Cosm ook niet. En van Let's Grow weet ik het ook niet. Kan zijn dat ze daar ook afwijken, maar dan echt qua visie gewoon.

I: Daar heb je niet genoeg zicht op?

R: Nee, ik weet niet precies hoe het daar werkt. Het lijkt me aan de ene kant sterk dat als je daar data stalt het meteen voor iedereen zichtbaar is, aan de andere kant lijkt het me ook sterk dat ze daar een sharingmechanisme hebben ingevoerd.

I: Want Let's Grow is voor kassen?

R: Het is van Hoogendoorn, die hebben Let's Grow eind jaren negentig gemaakt volgens mij.

I: En dat was dan in de tijd dat je een kastje in je kast hebt, een meetapparaat?

R: Het upload gewoon alle informatie die je in je klimaatcomputer hebt. En daar maken ze pdfs van, van die grafieken.

I: Denk je trouwens dat – hij staat niet hier in het netwerk – dat op de website duidelijk verteld wordt?

R: Het wordt er wel op beschreven ja, maar of dat duidelijk is. Dat zou je misschien op een nettere plek kunnen doen.

I: Hoe zou dat beter kunnen?

R: Ik denk sowieso dat de Sense website wel duidelijker kan, maar er zouden een paar steekwoorden op de voorpagina wat kunnen wat Sense doet, wat common Sense is en dat jouw data jouw data is.

I: Heb jij eigenlijk met de website te maken?

R: Inmiddels helemaal niet meer. Ik heb het origineel gebouwd ooit, maar inmiddels doet STAFF1 het.

I: Volgens mij zit ik wel een beetje aan mijn vragen. Denk jij dat ik nog dingen mis of heb je dingen die je heel graag wilt vertellen nog?

R: Nee, volgens mij niet echt.

## C.2. Developer 2

[936\_0301.mov]

I: ja hij doet het. Wat we gaan doen is we gaan eens kijken hoe het netwerk van Sense eruit ziet. met betrekking tot mensen en ook objecten dus eh ook eh producten zoals software en van alles en hoe dat dan vanaf Sense met andere bedrijven andere organisaties andere mensen

samenhangt en dan vervolgens gaan we kijken hoe er in dat netwerk eigenlijk het begrip privacy zich bevind en hoe dat ja of daar problemen tussen zitten qua mensen die in dat netwerk zitten en andere mensen in dat netwerk als die tegensstrijdige ideeën hebben en is dat een probleem ja nee. maar daarvoor wil ik eerst dus het netwerk hebben. En daarvoor wil ik vragen of jij op het bord in het midden een dingetje kan tekenen wat dan jou moet voorstellen je mag een poppetje tekenen je mag een stip zetten jij mag in ieder geval in het midden

R: okay dit ben ik

I: en zou jij links in zeg maar een beetje de linkerbovenhoek de top drie aan mensen binnen Sense kunnen neerzetten waar jij het meest te maken hebt qua werk

[01:30]

R: Nog een kleur, is dat handig?

I: ja dat mag je zelf weten

R: okay dan doe ik dus eh links top drie mensen met wie ik te maken heb?

I: ja

R: dat is vrij makkelijk. Ik stop moet ik erg geordend zijn?

I: nee hoeft niet geordend zijn mag gewoon eh

R: okay dat is mooi dat is makkelijk

I: Dus DEV4, DEV3, STAFF3

R: Ja

I: ehm en zou jij rechtsboven neer kunnen zetten met welke producten of diensten van Sense jij te maken hebt.

R: drie weer?

I: nee je mag zelf verzinnen hoeveel. Maar meer zo van wat eh ja waar jij mee bezig bent qua werk dan denk ik ja

R: producten en diensten

I: Ja is dat jij bijvoorbeeld bezig bent met de sport app

R: ja okay

I: Of dat jij bezig bent met het ontwikkelen van commonsense ik weet niet precies wat jij allemaal

R: ja ik kan er wel een paar dingetjes neerzetten. okay is eh (schrijft op het whiteboard) Niet producten of diensten naar buiten toe he? denk ik

I: ik weet niet wat voor dingen naar binnen toe waar jij mee bezig bent

R: ik heb een aantal dingen gewoon werken aan een platform dingen die gedaan moeten worden

I: dat mag erbij ook hoor dingen

R: okay

I: dingen waar jij tijd gewoon aan besteed wat met Sense te maken heeft zeg maar of wat voor Sense of binnen de tijd van Sense gedaan wordt. misschien heb je indoorlokalisatie

[04:00]

R: dat is net wat ik op wou schrijven ja

R: moet ik groter schrijven?

I: nee dat komt wel goed hoor

R: okay. nou dan kunnen we er nog wel eentje opnoemen denk ik

I: er komt zo nog veel meer bij hoor dus dat eh

R: o ja dan kan ik het ook hier bij laten

I: en dan aan de linkerkant links midden ongeveer o ja er moeten ongeveer zes clusters aan dingen komen. links midden wil ik graag weten met wie jij te maken hebt of met met wat jij te maken hebt wat zorgt voor communicatie naar buiten toe van Sense.

I: wat zorgt voor communicatie naar buiten toe.

R: Niet met buiten maar wat wel?

R: dat is bijv de website of communicatie mensen die zeg maar het bedrijf Sense verkopen of uitstralen. of

R: okay mensen of middelen met wie ik te maken heb die dan weer vervolgens naar buiten gaan, klanten of iets dergelijks

[05:15]

I: of als jij zegt ik schrijf zelf elke week een weblog daarin vertel ik hoe geweldig Sense is dan is dat ook prima

R: is niet beter een website. Is het heel belangrijk dat die communicatiekanalen niet mensen zijn



I: nee hoor je mag ook die mensen hebben. Dat is ook prima  
R: ja communicatiekanalen naar buiten nou ja dat is makkelijk dan noem ik gewoon STAFF3 omdat die er is. andere communicatie kanalen ja naparte van Sense  
I: mag ook  
R: die heeft wat Almende  
I: dat is ook prima  
R: maar dan moet ik niet mezelf hebben want  
I: nee jij zelf heb je al maar stel jij eh  
R: ja  
I: waar zat jij over te denken  
R: nou ik zat eerst te denken aan de indoorlocalisatie  
[06:08]  
R: maar dat is een meeting. een skype meeting telt dat als een apart middel?  
I: skype meeting eh  
R: of is dat weer gewoon een meeting maar dat telt niet  
I: ik denk niet dat een skype meeting telt ik denk wel dat de gene met wie jij die skype meeting hebt telt als iemand die Sense kan observeren, zeg maar een externe partij die met Sense te maken heeft als je daar partijen van hebt mogen die de rechterkant  
[06:30]  
R: ja die zijn redelijk gekoppeld aan een product in dit geval. ik kan van iedere  
I: oh zet maar achter elk product een naam van een clubje of bedrijf of aan mensen als jij wil die daar mee te maken hebben  
R: iphone app dat is gewoon gebruikers dat is anoniem. iets dat ik heb gebruikt eh  
I: hoeveel gebruikers heb je daarvoor voor de iphone app  
R: dat is heel lastig in te schatten  
I: okay  
R: dat kan ik geloof ik wel ergens zien maar ik heb geen idee hoeveel het zijn er niet zo verschrikkelijk veel maar het zal me verbazen als het er meer dan honderd zijn dus maar hij dient ook als de basis voor al die andere dingen maar ja ik communiceer hier bijna niet mee behalve dan dat ik dan schrijf en updates doe  
[07:34]  
R: ehm hoe heet dat eh iemand iemo, indoorlocalisation dat is van almende. ik had nog wat bedacht  
I: iVitality is zelf ook samen met DEV3  
R: die hoort wel hier niet helemaal maar wel gedeeltelijk  
I: ah ja  
R: maar ik zal nog even de Simon Sense erbij zetten de Jump App  
I: hihi  
R: en dat is, moet ik dat helemaal uitschrijven dat gaat niet passen. AliensAreAmongUs zo maar ja we waren hier bezig  
I: we waren daar bezig met communicatie kanalen middelen mensen die zich maar zich bezig houden met het communiceren van Sense naar de buitenwereld  
R: dus dan kan ik hier bijvoorbeeld de appstore neerzetten. dat is een middel waarmee we met gebruikers communiceren  
I: eh ja dat kan wel  
R: weet niet wat jouw bedoeling is. Dat moet jij zeggen, even kijken appstore zou kunnen maar ja je kan daar natuurlijk. je zet daar wel teksten bij van wat het is toch  
R: je zet er nieuwe kreten we kunnen nu dit en dat  
I: ik zou het er gewoon neerzetten dat is wel interessant  
R: via wat communiceer ik nog meer? ik zet geen nieuwsbrieven op de website  
I: zijn er wel eens artikelen over een van de dingen waar jij je mee bezig houdt gepubliceerd ergens of interviews.of  
R: Er is een keertje nee ja ik weet we hebben contact met iemand van deteraan ofzo die heeft een keertje wat gedaan over ontzettend algemeen en dan een beetje iPhoneApp die heeft nog ons toegezegd dat hij nog een een keertje iets over het fitness centrum gaat doen als we daar iets leuks van gemaakt hadden.

I: daar ben jij niet heel direkt bij betrokken dan of wel

R: nee de inhoud van het programma heb ik totaal, het enige waar ik is hier is de app, geen invloeden. middelen waarmee

I: Het gaat wel om dingen inderdaad waar jij zelf een beetje invloed op hebt maar als dit het is het hoor voor jou

R: denk het wel ja. ik doe niks op de website ik blog niet.

[10:46]

I: ehm effe kijken partners klanten eindgebruikers dat staat daar. Weet jij of er concurrenten of concurrerende bedrijven voor Sense zijn en zo ja welke en zou je die rechtsonder ergens willen zetten

R: rechtsonder. ik weet wel dat ze er zijn ik heb er ook naar gekeken maar wil niet zeggen dat ik de namen nog weet, dat is lastig he

I: je mag ze ook opschrijven als concurrenten dat is ook prima en zijn ze dan voor het Sense platform algemeen of zijn ze dan voor een van je toepassingen

R: ja dat heb je verschillende dat ligt ook een beetje aan je hebt ook een heleboel bijvoorbeeld voor het de activitySensor, dat zouden concurrenten zijn, zoals FitBit, of MapMy, enzo

[11:32]

I: ja. die doet dat ook niet automagisch toch of wel?

R: dat is het punt FitBit doet dat dan weer wel maar die geeft een overview van je data, dat is misschien wel competitief

I: nou zet er maar bij

R: ik kan hem wel FitBit

I: nou FitBit

R: commonsense in algemeen matig ik weet ook niet hoe die heet ik doe wel drie mooie puntjes zo

I: ja

R: ja en dan heb je nog zo'n bedrijfje en dan zijn er ook nog mensen concurrenten / samenwerken partner zouden kunnen zijn dat ligt er maar net aan wat je kunt met samenwerken

I: maar als ze dat niet willen

R: maar als je net een beetje half overlapt natuurlijk dan kun je of wel samenwerken of je kunt tegenwerken en dan ben je concurrent

I: Heb je daar namen van of die je er neer kunt zetten

R: nee, je zou kunnen zeggen google

I: je mag ze neerzetten hoor

R: ik weet niet of dat

I: ja

R: en de researchers zijn meestal geen concurrenten die maken een keer wat en dat is het

I: heb jij veel met researchers te maken gehad

R: valt wel mee alleen via papers

I: ja okay

R: als ik ze lees

I: okay

[13:45]

I: voor het beleid van Sense of waar Sense zou moeten staan in de markt zeg maar daar zijn bijvoorbeeld dan die concurrenten die geven wel een beetje aan van kijk ik kan hier of daar wel in de markt zijn want daar is nog niks voor gedaan maar als je dus concurrenten hebt die precies hetzelfde doen als Sense dan kun je zeggen van ja dat is niet zo'n handige plek om te zijn. Wie zijn daar nog meer bepalend voor het beleid en de plek in de markt van Sense denk jij

R: qua bedrijven

I: nou nee niet perse bedrijven bedrijven mag ook maar het mag ook mensen binnen sense zijn zeg maar wie er het beleid schrijft eigenlijk hoe het in elkaar zit

R: zal ik die boven neerzetten gaan we weer naar mensen die maak ik groen

I: mensen maak je groen dat is goed

R: ja mensen en bedrijven

[14:38]

I: dat is goed

R: de markt ik kan niet zeggen STAFF3 en STAFF2 dat zijn allemaal mensen die behoorlijk invloed hebben

I: nou ja doe maar gewoon onder middle worse want bij FitBit enzo want die hebben allemaal te maken met beleid maken

R: doe ik die hierbij

I: ergens onder lijkt me prima

[15:00]

R: Hier STAFF2 en STAFF3 ja wordt natuurlijk ook beïnvloed door anderen op het bedrijf dat moment

I: Dan zet die er ook maar bij gewoon dochterbedrijf Almende

R: ja

I: Dus eigenlijk ware het het Almende geheel heen gaat bedoel je dan

R: Ik zet er het Almende imperium neer

I: dat is goed

R: maar die hebben toch wel invloed want dat is daar zijn vaak ook meteen klanten of via wie we weer projecten hebben met anderen. zo

I: okay

R: zijn er ook nog meer of andere bedrijven juist. de anderen zijn wat indirecter als je er mee contact hebt ja dan. Je hebt nog detlab bedrijven

I: detlab mag ook ja

R: die invloed is niet zo heel groot. maar je hebt natuurlijk wel als detlab met iets komt wat dan weer mooi aansluit ook wat we aan CommonSense kunnen koppelen

[16:20]

I: Dan zorgt dat voor werk

R: ja

I: En maakt dat dus wat jij ontwikkeld als bedrijf

R: er zijn er vast nog wel meer

I: Weet jij of het beleid van Sense eigenlijk ergens in documenten is vastgelegd of dat daar ergens

R: Nee niet dat ik weet. Volgens mij zit dat vooral in de hoofden van STAFF3 en STAFF2. Dat er beleid is vastgelegd als het er is daar weet ik niets van

I: Dus een visie van waar zouden we zijn met Sense over vijf jaar bijvoorbeeld

R: Ja die bestaan wel.

I: Die bestaan wel

R: Volgens mij wel. Op de jaarlijkse bijeenkomst ging deels ook daar over. En die daarvoor waar ik natuurlijk niet bij was. zal ook wel bedacht zijn ...

[17:20]

I: Zou jij de jaarlijkse bijeenkomst daar neer kunnen zetten. als ook een middel of een

R: ja

I: En dat is de jaarlijkse bijeenkomst waar dan wordt bepaald wat gaan we doen met Sense dit jaar.

R: ja, beetje evaluatie en wat gaat er gaat komen wat er te koop is en waar meer mogelijkheden

I: Maar je zegt vooral STAFF3 en STAFF2 zijn belangrijk voor de visie

R: ja ik kan zeggen alle mogelijke klanten zodra je ze tegen komt, maar dat is een beetje flauw. natuurlijk ook deels technologie dat is ook een hele belangrijke hee er zijn nieuwe telefoon er zijn nieuwe mogelijkheden bluetooth energie mogelijkheden voor medische apparatuur hee dan doe je dat

I: technologie mag ook. Ik vind het allemaal mooi

R: ja des te meer des te beter he

I: Ik moet eens even kijken wat er uit het gecombineerde plaatje komt

R: ja je krijgt natuurlijk overlappende dingen

I: Daarom zeg ik dan schrijf maar zoveel mogelijk op wat je denk. Behalve dan bij de medewerkers want als je daar zegt van eh schrijf maar iedereen op. ja dan krijg je gewoon een

R: ja dan krijg je van iedereen, het bedrijf is niet zo groot dat je niet iedereen zou kunnen kennen

I: ja

R: Die technologie van net die hoef ik niet op te splitsen denk ik

[18:58]

I: als de technologie iets nieuws biedt waar je als bedrijf heen kan. Dat was het stukje delen van een netwerk.

R: Dit zijn de nodes

I: Dit zijn de nodes nee je hebt nog geen netwerk maar eigenlijk zijn alle nodes dus verbonden met jou.

R: ja

I: Behalve misschien de concurrentie die zijn alleen maar verbonden met jou in de zin van dat jij weet dat ze bestaan maar daar heb je niet wekelijks overleg mee en dat soort dingen.

R: nee,zelfs helemaal geen overleg

I: nee. Dit is voor zover het netwerk in kaart gebracht moet worden. Of heb jij nog zeg maar, want eigenlijk staan al die notes met jou in verbinding, heb je nog ideeën of die notes onderling nog heel veel met elkaar in verbinding staan

R: o ja,dat doen ze zeker

I: Wie en wat staan er vooral met elkaar in verbinding?

R: Nou de eerste is een hele flauwe, deze [wijst naar medewerkers] staan met elkaar in verbinding. Deze projecten zeer zeker ook. iVitality daar reken ik ook een beetje samen met iemo.Dat valt er eigenlijk ook een beetje onder zelfde doel medische toepassingen, dat is hier ik denk dat ik wat te tekenen heb dat is ook leuk

[20:01]

R: directionele verbindingen?

I: dat mag.maar je mag het ook gewoon

I: Als het echt heel nodig is om daar richting aan te geven dan kan dat natuurlijk. De relatie js op zich er wordt niet direct iets gezegd van die geeft iets aan die

R: dat kan als jij daar iets mee gaat doen dan gaan we dat proberen natuurlijk. Even kijken wat deze onderling. Deze is dan wel weer een beetje flauw maar dat gaan we toch eventjes doen. Ik had hier beter een bus voor kunnen gebruiken

I: ja, zo'n iphone app is overal voor belangrijk ja. dat is gewoon de backend iphone of nou ja

R: framework platform

I: framework

[21:30]

R: ja inderdaad ik heb een beetje twee dingen gecombineerd die eh framework, en de app waarmee eigenlijk direct aan wordt gewerkt

I: Dat is zeg maar vergelijkbaar met de android app waar je gewoon kan zeggen ik doe die sensoren uitlezen

R: Ja de android app kun je ook gebruiken gewoon in een ander projekt. Ik doe eerst even per component

I: ja

R: deze kan ik ook gaan doen maar

I: ik denk niet dat die heel erg

R: deze weet ik niet

I: Het is vooral interessant om te kijken of er tussen die groepen connecties zitten

R: oke o ja

I: Jij hebt STAFF3 op drie plekken staan dus die zal vast wel goed verbonden zijn

R: dan zou ik bijvoorbeeld kunnen zeggen [trekt streep van DEV3 naar iVitality en praat in zichzelf streep van FitBit naar activity Indoor localisation, ja, dat valt mee. Natuurlijk, STAFF3 coordineert dat een beetje maar] heeft deze iets te maken daarmee eigenlijk niet zoveel vind ik. Het enige wat ik kan doen Ik kan zeggen waar we mee concureren als connectie.

[23:15]

I: dat zou kunnen

R: maar er is eigenlijk maar een redelijk mogelijk direct competitor.

I: hm hm

R: dat doen we zo. deze met andere dingen is ook een beetje te

I: dat wordt ook te compleet

R: Deze hebben we zo'n beetje allemaal hier.

I: Die krijg ik ook wel door interviews met hun te houden

R: Deze met die dat ja dat kan ik wel doen maar

I: Dit is eerst ook wel mooi hoor  
R: o ja ik heb hier weinig backend opgezet dus dan heb ik weinig DEV4s erbij  
[24:00]  
I: Maar als jij je niet heel veel bezig houdt met backend ontwikkelen dan eh  
R: Nou ja dat is een beetje voor mij waar ik naar toe gaan ben. Ik ben de laatste tijd wel bezig op de backend zodat ik er wat meer van weet en er wat meer mee kan doen  
I: je mag het er neerzetten hoor. backend Sense  
R: Ja die zet ik er gewoon bij. Lekker compleet  
I: Dus dat is commonsense, API achtige dingen  
R: ja en backend patroonherkenning, die ik graag op de backend wil doen. States herkennen.  
I: ja  
R: backend heeft communicatie niet met deze direct nee. okay  
I: ja die software rapporteert waarschijnlijk aan de backend  
R: Nu STAFF3 zo'n connector is is die met moeilijk niet. Ik kan bijna zeggen STAFF3 is natuurlijk ergens op de een of andere manier met al die projecten betrokken.  
I: Het is niet echt zo of jij met STAFF3 samen aan zo'n project werkt of wel? Want met DEV3 zul je waarschijnlijk overleg hebben over iVitality  
R: ja met nee met STAFF3 niet. wacht we hebben wel met de indoorlocalisatie meetings op dit moment samen met STAFF3 waarschijnlijk omdat hij de vaart erachter wil houden  
I: ah is prima  
R: ja  
I: ja hoor  
R: nog nieuwe dingetjes

## Privacy

I: Nu gaan we vragen stellen over privacy.  
R: Okay dat is goed ben ik wel benieuwd naar  
I: Je gaat je zelf overnieuw tekenen  
R: Ja ik vind dat ik er toch niet helemaal goed eh uit kom dus. Ik moet minstens kleurrijk hier erin zitten. Dat ben ik.  
I: okay  
R: okay, gaan we het hebben over privacy.  
I: over privacy  
R: moet ik bij het whiteboard  
I: nee hoor dit mag gewoon aan tafel hoor. Wat is volgens jou privacy  
R: privacy. Wat is de definitie van privacy  
I: ja, of wat jou perceptie is van privacy is wat vind jij wat privacy is en dan misschien in relatie met wat er bij Sense gebeurt  
R: Mijn idee van privacy is het niet kenbaar maken van bepaalde informatie aan meestal derden. Met als je samen met iemand iets doet dan heb je meestal heel snel dat je beide over informatie beschikt. Maar het vooral niet kenbaar maken van informatie eigenlijk aan derden. Mensen die er niet bij betrokken zijn dat zij daar ook niks of bepaalde dingen niet van weten. Dat is voor mij wat privacy inhoudt.  
I: okay  
R: of moet ik daar nog op doorgaan  
I: Ga maar gewoon door dat is prima  
R: In verband met Sense is dat natuurlijk een hele makkelijke dat wij gegevens opslaan en die komen op bedijfsservers terecht. Waarbij we niet alleen toegankelijk zijn voor de gebruikers om wie het gaat maar in principe ook voor ons of voor anderen via ons. Of gewoon als wij ook via ons dan zijn wij ineens beschermheer van hun gegevens.  
[28:03]  
I: ja  
R: Ik vind dat op zich wel een belangrijk punt om mensen dat mensen zelf kunnen aangeven wat we met hun privacy doen. Dat het echt van je zelf is. En dat je geen publiek bij maken dat is oke. Maar het feit dat je de Sense app gebruikt moet niet betekenen dat je ook je gegevens moet publiceren of laten gebruiken door anderen. Ikzelf wil nog wel eens informatie weggeven vooral

aan mensen die ik ken maakt me niet zoveel uit maar ik vind het wel belangrijk dat je een soort zelfbeschikkingsrecht hebt.

I: ja

R: ook met al die onzinnige dingen waarmee ze het liefst proberen door te voeren via europesche regelingen dat een handtekening onder een mailtje dat er daar  
[29:20]

I: jah. Dus voor jou is privacy dat je het recht hebt om als jij informatie over je zelf verzameld hebt dat jij zelf mag bepalen voor wie die informatie beschikbaar is.

R: ja dat is je zelfbeschikkingsrecht over je informatie dat anderen informatie over jou verzamelen en Sense verzameld informatie over iemand dat doet ie zelf. Maar als ik iets meet waar jij ook bij betrokken bent

I: ja

R: dan wordt het natuurlijk wel wat lastiger want is het mijn data is het jouw data

I: Stel jij meet nu dat mijn bluetooth aanstaat op mijn telefoon en jij weet dat ik bij jou in de buurt geweest ben

R: precies is dat mijn informatie is dat jouw informatie. Is dat eigenlijk wel iemands informatie. Dat wordt een lastige. Ik weet niet helemaal zeker wat ik

I: Wat je daar van vindt

R: ja wie of wat daar beschikkingsrecht over moet hebben. In principe moet je niet zo kinderachtig zijn en moet je wel informatie kunnen delen. Zolang het niet direct iets over iemand anders zegt. Je mag best zeggen dat het hier druk was veel gepraat werd, ja dat zijn allemaal informatie ja dat eh

I: ja

R: Het behelst mij maar niet heel specifiek voor een ander. maar ook inderdaad ik kan niet zeggen mag niet zeggen dat ik hier met Roelof gepraat heb. Dan koppel jij jou er aan dat wordt iets complexer want dat waren twee belanghebbenden.

I: ja

R: Hoe je dat moet delen dat weet ik niet maar dat is ook iets wat je via technologie steeds makkelijker kunt delen.

R: Ja dat weet ik niet hoe je dat tot een oplossing zou daar moet je gewoon iets voorzichtig mee zijn de maar wat dan de juiste verhouding zijn de manier van wat mag wel en wat mag niet

I: Als je nou data verzameld als Sense zijnde en die beheer jij dus voor persoon X

[17:20]

*[93010301.mov]*

I: Hoe denk je er dan over als Sense zegt van ja weet je wij vinden dat bedrijf Y daar ook wel aan mee mag doen met die data dus dat eh

R: dat er gebruikt wordt gemaakt van die gegevens dan zeg ik meteen maar doen want alleen opslaan dat is een beetje nodeloos, daar moet echt wat mee gebeuren maar dat is eigenlijk een zaak tussen bedrijf Y en de persoon zelf daar is Sense eigenlijk niet direct bij betrokken behalve dat zei het mogelijk kunnen maken om zo iets te doen.

I: ja okay

R: Ik kan me voorstellen dan een aantal van die dingen via Sense zouden gaan dat ze bijvoorbeeld zeggen wij hebben een partner hun hebben leuke onderzoek en dat je als gebruiker denkt, he niet wee. dan leer je ze kennen maar dat gaat dan altijd eigenlijk tussen de gebruiker zelf en diegene die er gebruik van willen maken. en goed natuurlijk kan je daar een faciliterende rol in hebben maar dan alleen faciliterend maar niet

I: niet dat jij zegt wij hebben honderd gebruikers hier mag je de data hebben

R: nee. Er moet wel instemming zijn.

I: moet wel overeenstemming zijn dus

R: ja het hoeft dan niet heel met handtekeningen en alles maar gewoon dat kan wel heel simpel zijn. we doen nu een experimentje, je moet deze app downloaden en als het dan maar duidelijk is dan ga we naar die data kijken want je zegt nu opeens gebruik het maar dat vind ik wel dan heb je zelf beschikking en hoeft ik niet deel te maken het maakt niet uit.

I: vergelijkbaar met zeg maar het toestemming geven voor toegang tot je informatie zoals dat bij facebook apps gebeurd zeg maar zoiets

R: nee misschien mag ik daar nog iets nee

I: maar

R: zodra je het niet gaat gebruiken in dienst waarvan je redelijk van verwacht he

I: he die gaan iets met die data doen

R: die gaan iets met die data doen als het gewoon duidelijk is dan is dat al genoeg hoeft niet helemaal dichtgetimmerd met een overeenkomst als het maar duidelijk genoeg is. transparantie is heel belangrijk

[02:30]

I: en nou is het natuurlijk dat we hier voor het ontwikkelen van allerlei toepassingen dat wil zeggen nou weet je wat we pakken alle mogelijke sensors die we hebben om te kijken om te kijken of die wat over jou kunnen vertellen. Vind jij dat dat zeg maar in uiteindelijke produkten ook zo zo moet zijn, zeg maar dat alle sensor informatie bij elkaar moet of dat dat allemaal verzameld moet blijven ook als zou het niet relevant zijn voor wat voor toepassing dan ook maar. Stel je voor je verzamelt lichtintensiteit van waar je telefoon is geweest en dan blijkt dat je eigenlijk nog niet echt een toepassing hebt gevonden voor lichtintensiteit

R: ja maar waarom ben je dan licht de gebruiker is lichtintensiteit aan het verzamelen. Wij niet in principe dat is het idee.

I: jaah

R: Het lijkt er wel op dat wij toegang zouden kunnen krijgen. maar Ik weet ook niet hoe ja dat dan zou moeten oplossen en wat de mogelijkheden zijn om dat met cryptografie te doen lijkt maar ik wil ook weer delen met anderen ik weet niet hoe we dat goed op kunt lossen

I: Op dit moment kan Sense zeg maar bij jouw data als gebruiker

R: ja dat is het uiteindelijk noodlot

I: is dat heel moeilijk of hoe eh

[03:55]

R: nou het punt is je kunt dat dicht timmeren inderdaad maar dan wordt het wat lastiger want goed het is heel makkelijk om gewoon data op te slaan als zijnde nou dit is data dit is de sleutel klaar. je zou wel gewoon op de telefoon de sleutel kunnen toepassen

I: ja

R: en dan de key eveneens gebruiken maar vervolgens ga je die data delen en dan moet er ook een key zijn waarmee anderen toegang geven moet laten geven op key data nou dat is op zich okay dat kan dan kun je anderen toegang geven tot die data dat gaat nog wel denk ik maar op het moment dat je de key weer opnieuw wilt intrekken dan wordt het al wat lastiger dan zou je er op de een of andere manier voor moeten zorgen dat je iets met die keys eh

I: je zou je data opnieuw moeten versleutelen ofzo als het ware als je dat wijzigt dat wordt lastig [05:00]

R: En als iets interessants doet zoals een algoritme dat die data correleert en er iets mee doet dat heeft ook ergens een sleutel nodig.

I: ja

R: en op dit moment is het zo dat die algorithmes vooral bij Sense draaien dan komt de ...niet bij Sense en zullen dus altijd waarschijnlijk bij een third party draaien

I: ja

R: tenzij je natuurlijk de telefoon op je eigen computer zou draaien maar dat ziet er nog niet echt zo naar uit dus dat wordt lastiger want je wilt ook wat kunnen toevoegen aan iedereen en daarvoor hoef je der niet als mens in te zien maar wel met een algoritme dat wel fijn

I: Dus als je bijv. van alle gps traces van mensen bij elkaar een wegenkaart zou willen maken.

R: dan wordt het al lastiger want er zijn algoritmes die bijvoorbeeld kunnen werken met verschillende gegevens en dat dan uiteindelijk niemand weet ...specifiek maar dat staat een beetje in de kinderschoenen en dat zijn hele trage algoritmen en ik weet ook niet of ze ook altijd toepasbaar zijn. Maar er zijn ontwikkelingen die kant op nou ja als wij dat niet zouden proberen toe te passen denk ik dat we qua performance niks meer kunnen en het ligt er aan als je gewoon de data van een persoon wil om te correleren dan weet je altijd de data van die persoon. dus dan en als ik het niet weet is het ook waarschijnlijk dat wij er gewoon bij zouden kunnen.

[06:23]

I: ja. ehm met het denken over privacy zoals jij zeg maar vindt wat privacy is en wat er zou moeten met privacy hoe denk jij dat alle elementen die jij in je netwerk hebt getekend hoe die daarover denken. Zijn daar partijen die echt heel erg anders over denken over privacy of die het

juist heel erg eens zijn met wat jij vindt?

R: Nou ik denk dat iedere afnemer van data een researcher die heeft als eerste insteek van wij willen wat met die data privacy dat is misschien belangrijk omdat hij graag die gebruiker wil houden maar die wil over het algemeen eerst vooral de data. Dat is wel een conflict, maar dat wil niet zeggen dat ze niet open staan voor privacy maar hun eerste belang is gewoon die data en hoe dat met privacy zit is een gewoon een tweede orde probleem.

I: ja dat is gewoon een voorwaarde om te zorgen dat je überhaupt respondenten krijgt voor je onderzoek zeg maar

R: ja maar misschien vind je het wel belangrijk zeg maar maar in eerste instantie wil je met die data gewoon wat doen. Als wij zeggen oh je hebt de data dan zeggen ze dan jip we zijn tevreden denk ik

I: wie zou jij in deze tekening rekenen als researchers? dan in die zin

R: data afnemers dan zou ik even kijken of ik een mooi kleurtje

I: ja je hebt alles al een keer gebruikt he?

R: ja dat geeft niet. Dan doen we gewoon contrasterende kleurtjes ondertekenen. iVitality is bijvoorbeeld eentje die wacht even afnemend van data indoorlocalisation dat is eigenlijk een project waar we mee bezig zijn en nog niet echt uiteindelijk zal dat ja wat moet ik zeggen op dit moment eigenlijk niet op dit moment zijn we nog gewoon aan het experimenteren en dan laten we inderdaad en voor ons zelf laten we de privacy lekker zitten. dat is wel zo. Wat zij met data willen dat zijn wel een hele flauwe afnemer [activitySensor]. Deze is zijn ook echt wel afnemer van data die horen er echt wel bij. deze [iPhone App] zijn gewoon dat is mijn eigen data dat zijn niet de serieuze afnemers, en voor hen zou het zo flauw zijn dat je hebt dit zou weinig met privacy te maken hebben.

[09:17]

I: Aggregeren die zeg maar die tijden die je nu onderstreept hebt aggregeren die ook data van verschillende gebruikers bij elkaar?

R: ja.als je kijkt gewoon per gebruiker maar ze hebben bijvoorbeeld allemaal een controle groep nodig voor hun experimenten. als je kijkt naar hoe varieer je dat die variatie iemand de groep binnen andere bedrijven alleen maar om voor een persoon iets te detecteren, te zeggen jij moet ook weten wat de norm is wat voor andere mensen geld is.

I: ja

R: Op die manier moet je het ook zo doen

[09:55]

I: oh dus dan kijk je bijvoorbeeld voor die activity sensor, zeg je van eh nou dus een heleboel mensen zeggen dat fietsen dat dat bij dit patroon past dus als jij iets doet wat hier op lijkt dan zal het waarschijnlijk fietsen zijn

R: dat kan. Daar ben ik wel mee bezig op dit moment is dit vooral de digitale invoer die dit dat kan alleen maar dat voor andere mensen zijn. maar het is ook bijvoorbeeld zijn gebruiker bijvoorbeeld echt wat we nu ook gewoon meteen doen is zeggen van he we maken kaarten he jullie moeten daar zoeken omdat julie de hoeken zijn van allerlei fundamenteen jij bent handig he wij willen vinden het oke dat je ...wandel fiets en ...dus die ja dat soort manieren wordt het gewoon geaggregeerd

[10:43]

I: okay

R: met meer.

I: oh

R: moet ik nog meer

I: nee je mag er nog meer zeggen

R: wat heeft er nog meer te maken met meer data afnemers of gerelateerd aan privacy

I: ja

R: concurrenten zijn niet echt onze data afnemers natuurlijk althans niet voor zover ik weet. Want ik heb ook ...staan ergens okay. Dit zijn deze [groen rijtje middenonder rechts] verschaffen eerder data dan dat ze afnemer zijn. nee ik vind dit echt wel de voor mij waar ik mee te maken heb eigenlijk de grootste echt data afnemers.

I: okay das goed

R: Praat maar door hoor



## Covenant

I: yes met een legenda. Wat ik dan eigenlijk nog wil weten is eh. Stel je voor jij zou vanuit Sense mogen bepalen wat jij eigenlijk naar de buitenwereld toe zou willen beloven met betrekking tot privacy. Zodat jij zegt van alle software en alle produkten en diensten die wij leveren daarvan kun je ervan uitgaan dat wij dit wel doen dat niet doen. wat we allemaal dan eh

R: Nou De eerste en aller belangrijkste in beloftes zouden zijn transparantie Dan wil ik zeggen van oke je weet wie je kandidaat je weet welke data je deelt met anderen en welke niet. wat er gebeurt in de database de transparantie dat is want alleen daaruit kun je vervolgens beslissingen gaan maken. Zolang je niet weet wat er mee gebeurt of als we daar niet doorzichtig in zijn, dan ...vinden dan is transparantie ook heel belangrijk. Oh je vroeg net ook nog wie het met me eens was

I: oh ja oh maar dat kan hier na ook hoor

R: okay

I: dit komt ongeveer op hetzelfde

R: Een andere belofte ja een andere belofte bijvoorbeeld is: je houdt je eigen beschikkingsrecht dus dat geef ik niet aan derden die informatie en eigenlijk hoort daar ook nog wel bij dat we zelf die informatie ook niet gebruiken. Behalve voor, nou wat nodig is omdat we bijvoorbeeld een dienst aanbieden en die maar verder niet dat we het voor iets anders gebruiken dan waarvoor je denkt dat we het gebruiken. Dat je niet ineens zomaar omdat je toevallig vaak in Nederland ben bepaalde advertenties hebt.

[13:45]

I: nee okay. Is dat dan ook omdat jij zegt medewerkers van Sense moeten er uberhaupt niet in kunnen kijken of

R: ik vind in principe

I: Zou jij dat willen beloven zou jij dat zeg maar als jij Sense zou zijn zou jij dan zeggen dat is wel waar wij voor staan of waarvoor wij willen staan

R: Dat medewerkers niet in de data kunnen kijken.

I: ja

R: Ik denk dat dat goed is om daar, omdat te bekijken. ik denk dat dat ik zou wel willen zeggen wij kunnen niet bij de data dat zou ik heel graag willen ik denk niet dat dat realistisch is uiteindelijk. Maar het zou natuurlijk wel goed zijn om te zeggen oke wij hebben als er mensen zijn die bij de data kunnen wij daar niks aan kunnen doen. Hebben wij er een of twee nou

I: Zou je dan die mensen ook willen screenen van te voren ofzo dat ze betrouwbaar zijn met die data of dat je hoe eh

R: zucht. nee ik denk niet dat nee, nee ik denk niet dat dat de oplossing is het zin heeft om te screenen op mensen want dat betekent alleen dat wat ze in het verleden hebben gedaan en wat mensen doen, karaktereigenschappen zijn eigenlijk veel minder belangrijk dan de omgeving

[15:00]

R: Dan zou het eerder het systeem maken dat transparant is zodra iemand de toegang heeft dat je gewoon kan zien he iemand heeft gekeken naar eh

I: Dat je gewoon per keer dat de data bekeken wordt door wie dan ook maar dus ook door mensen aan wie jij recht hebt gegeven om te lezen dat je daar dan van kan zien he kijk die kijkt elke dag even naar waar ik ben

R: Had ik het fout binnen Sense toch

I: ja dat ging om binnen Sense naar te kijken. Ik neem wel aan dat dat kan.

R: Ik heb hier meer specifiek gezegd, als iemand de toegang tot de gegevens heeft als we dat dan netjes loggen en ervoor zorgen dat er dan dat we allemaal ook eventjes af en toe gekeken wordt voor mijn part zegt iedereen die heeft lopen neuzen in de data. Dan heb je sociale controle en dat zorgt ervoor dat we dat redelijk goed lukt. En om dat breder te trekken dan heb je ook meteen weer andersom, dat als iemand jou data gebruikt mag er over al dat gebruik van je data wil je weten wanneer iemand je gegevens heeft bekeken en waarmee dan, dan heb je weer gebruik van die ander

I: Dat zit een beetje in elkaar vast

R: in elkaars vaarwater

R: je kunt zeggen van je geeft anderen toegang en dan belangrijk is dat je dan ...over waar de ander toegang tot heeft

I: ja

R: Ik denk dat we, het is misschien leuk om inderdaad te zien he er zijn gebruikers die volgen mijn data maar dan zit je weer in andermans vaarwater het is belangrijker is ik weet precies dit deel ik met jou en of je dar nu wel of geen gebruik van maakt dat is weer wat anders maar in principe je mag gebruiken maar dat is belangrijker dan dat je er gebruik van maakt

I: Dus transparantie en het niet aan derden doorgeven van de data

R: Ja dat zijn eh

I: ja dat zijn de belangrijkste of heb je er nog een

R: sorry dat niet aan derden daarmee bedoel ik eigenlijk gewoon beloven dat iemand zelfbeschikking heeft. Het mag wel aan derden maar dat is niet onze keuze. Wij gaan er niet zomaar aan alle andere mensen

I: nee nee eigen beschikking is eigenlijk de titel

R: ja of zelfsbeschikking, zelf bepalen over de data dat lijkt me wel dat is eigenlijk twee qua privacy dingen als je weet wat er gebeurd en ook als je zelf toestemming daarvoor kan geven, dan is er eigenlijk weinig probleem meer

I: Dus als jij zeg maar die belofte wilt doen van transparantie van hoe die data gedeeld is en wie er allemaal naar kan kijken en het zelfbeschikkingsrecht van dat jij zelf mag bepalen wie er allemaal aan jou data mag zitten en naar mag kijken, dingen mee mag doen. Hoe denk jij dat dat zeg maar binnen jouw netwerk wat je daar hebt of dat mogelijk is om dat uit te voeren om dat zo te brengen. Denk jij dat dat alle elementen in dat netwerk op dit moment daaraan meewerken of daaraan voldoen zeg maar aan die eisen en eh

R: ja maar als ik begin met bij de tweede, waarbij activity sensor die data delen met PulseTracks, PulseTracks maakt vooral gebruik van facebook en in facebook heb je al het recht dat je toestemming kan geven, van je geeft nu toestemming en facebook kan daar zelf dan helaas ook weer van alles mee doen met die data dat is dan wel jammer maar aan de andere kant dat is wel in ieders geval eerlijk naar de gebruiker zegt oke wij gebruiken facebook wij willen die data ook op ons facebook beschikbaar hebben. Dus dat is je eigen keus

I: ja

[19:47]

R: iVitality, dat is meer onderzoeks gericht die willen die mensen uitrusten met die telefoon en voor en zij willen in die data neuzen eigenlijk onderzoek doen zien wat voor relaties ze doen. Het is belangrijk dat wij ze blijven faciliteren. dat de gebruikers zelf echt inderdaad zeggen he wij gebruiken deze app en we weten dat we daar vrije toegang toe krijgen. Het is ook een echte context vooral in deze staat dat zij in die gegevens gaan neuzen. Dat weet je dat is het hele doel van

I: van onderzoek doen ja

R: Dat is ook prima in dit geval kunnen we zolang de gebruikers het weten en ik denk dat ze het weten want ze hebben ingestemd, zo ergens met een handtekening

I: Stel dat de mensen ergens halverwege het experiment bedenken ik wil dit eigenlijk niet meer, is het dan ook mogelijk om te zeggen nou je krijgt nu geen toestemming meer om mijn data te zien en eigenlijk de data die je al had wil ik alleen maar voor mezelf hebben.

R: De eerste kan wel, weg ermee geen toestemming meer

I: maar dan ook niet voor data die je al eerder hebt eh

R: dat is bij ons lastiger. ik geloof dat er nu een knop was om de hele account te verwijderen. Ik weet niet helemaal wat daar de toekomst van is der was ook nog een hele account kunnen verwijderen maar in principe dat zegt nog niks want als hij de gegevens zou hebben

I: dan kunnen ze copien gemaakt hebben

R: een copie en moet je dat dan legaal gaan dicht timmeren van he met terugwerkende kracht. Ik denk dat dat te moeilijk is en ook dat ie dat nee ik denk niet dat dat iets is wat wij dat moeten ondersteunen Dat betekent dat je legaal gaat dicht timmeren van he als er resultaten zijn gebaseerd op jouw gegevens, wat moet je daarmee doen moet je die ook weggetrokken worden?

I: Dat wordt te veel

R: Eens gegeven is gegeven. Dat is wel zo je deelt dat is ook gewoon de digitale wereld waarin de hele tijd kopieen gemaakt kunnen worden Dat is gewoon hoe technologie eigenlijk werkt en het is digitaal en je kopieert het als het eenmaal iets op internet zet krijg je het er moeilijk weer af.

I: ja

R: ik vind het onzinnig om het te proberen met terugwerkende kracht te doen. En het is misschien ook niet eerlijk ten opzichte van diegene met wie je het hebt gedeeld. Wel als het gewoon totaal en vrijblijvend was

I: ja

R: maar op het moment dat je misschien enige overeenkomst hebt of toch wel duidelijk van he ik deel dit en vervolgens ben je afhankelijk van jou data en ineens met terugwerkende kracht wordt dat

I: ja dat is net als wanneer er bijvoorbeeld iemand jou van te voren een tentamen zou laten in kijken en dan zeggen van kijk kijk dit is het tentamen wat je morgen krijgt en dan zegt hij als je het gelezen hebt en ja nu heb je het niet meer gelezen want dat mag helemaal niet he Ik wil niet dat je het in gezien hebt. Ja dat werkt niet

R: nee

I: nee dat is inderdaad vrij lastig dan

R: In zo'n zin lastig dat je er eigenlijk niet aan moet beginnen. Het is onzinnig eigenlijk om dat te proberen.

I: ja. En verder qua eh misschien mensen in dat netwerk of bedrijven. Zeg maar zouden die jouw visie op privacy en op hoe je daar als Sense mee zou willen omgaan ondersteunen of zou je zeggen daar zitten bedrijven tussen die zeggen van ja dat is allemaal leuk transparantie en eigen beschikkingsrecht maar dat klopt bij hoe onze wereldvisie is

R: Met name met diegene met wie ik contact hebt Die zijn het er redelijk mee overeens dat je misschien laat zien hoe belangrijk je het vind. maar ik denk uiteindelijk ...ik kan me voorstellen dat er andere partijen zijn die daar andere partijen zijn die daar anders over denken en dan denk ik vooral aan gevestigde marketingsburo's om mee te beginnen. Die zijn het nogal gewend wat met die data te doen en het heel vanzelfsprekend vinden dat je data kunt verzamelen over mensen die browsen op de website. Ik denk dat zei het niet met me eens zijn, maar daar heb ik geen contact mee

I: Heeft Sense ook geen opdrachten bij lopen toch bij marketingburo's?

R: Volgens mij hebben we daar niks mee. We hebben we het een keer gehad dat we wel een interessante mogelijkheid je kunt de mensen koppelen die marketingburo's en mensen. Dan faciliteer je die twee en die zijn bereid tegen een vergoeding al dan niet gegevens te delen

I: ja

R: ik zie niet echt. Maar dat is ook deels omdat ik ben natuurlijk ook beïnvloed door mijn omgeving hier met hoe ik denk over privacy

I: ja

R: dat is logisch. En vooral als ik contact heb met klanten nou iVitality daar kwam ik later pas bij dus ik geloof dat we met STAFF3 wel redelijk hebben overlegd dat dat vanaf de gebruiker gebeurt. ik ben daar later bij geweest en dat hebben ze redelijk vast. En de activity sensor die moet samen met PulseTracks en ik heb het idee dit past gewoon netjes bij wat ze altijd anders al doen. De gebruiken willen ook geaggregeerde data ik heb het idee dat dat ook eh. maar ik weet niet zeker ik kan niet zeggen wat ik hoor of zeker weet wat zei met hun data doen ik niet honderd procent zeker Ze zeggen dat niet, maar ik weet niet

I: Is daar niet het inzicht wie er allemaal bij die data kan?

R: ja wel in dit geval de app die we daarvoor maken nog in mijn account en geeft vervolgens pulse tekst is een app op facebook die toestemming geeft

I: hm hm

R: dus op die manier geef je bevoegdheid aan iemand en toegang tot de app en toegang tot de gegevens daarnaast sturen wij die gegevens aan PulseTracks en niet aan facebook. Facebook is niet een site voor dit soort dingen die hebben meer een app voor denk ik en in dit weet je dat je je logt in bij pulsetracks je hebt een account bij hun lopen met een open privacy verklaring en wat daar bij hoort want ik wist transparantie is er zeker dat je met PulseTracks een contract hebt. [26:49]

I: okay

R: maar ik moet zeggen wij ik heb niet heel goed gekeken of dat wat er in precies het contract staat. Ik heb het idee dat wij daar eigenlijk vooral die gebruikers toegevoegde waarde willen dienen. maar zullen wel inkomsten ook nog hebben facebook site maar verder heb ik geen idee

dat ...maar weet het niet helemaal zeker

I: En in de backend zeg maar software technisch zijn die mogelijkheden er allemaal die jij zegt dat er moeten zijn. Dat duidelijk is van nou wie is nu die data wereld en dat die bevoegdheden intrekbaar zijn.

[28:15]

R: ja die backend is wel maar eigenlijk als gebruiker op dit moment. Als ik gewoon de Sense app en het Sense Platform gebruik als op de website dan is dat zeker nog niet wat het moet zijn. Qua transparantie, want je weet wat je op de website kunt zien is of je het gedeeld hebt wat op zich al goed is maar vervolgens deel je het een keertje met Jan en je deelt het een keertje met de groep en vervolgens deel je het met iedereen en vervolgens weet je alleen maar dat er gedeeld is.

I: Maar naar niet met wie

R: nee. Die informatie zit wel in de backend maar die informatie wordt niet getoond

I: daar is geen interface voor

R: Als gebruiker heb je er niks aan betekent dat alleen in de trend van dat je deelt. Niet met wie je deelt.

I: ja

R: En je kunt het wel ongedaan maken enzo, maar die interface is nog niet echt bruikbaar, nee

I: nee. ja Dus dat zou nog iets zijn wat wel nog nodig is om te veranderen voordat je eigenlijk die hele belofte die jij wil doen waar kan maken

R: ja zeker

I: Zijn daar verder nog grote hobbels of dingen die anders zouden moeten dan of is dit volledignog

R: Wat nog mogelijk een hobbel is maar wat ook belangrijk is; van die bescherming van gegevens:

I: hm hm veiligheid

[30:00]

R: ja veiligheid. Wij zeggen wij slaan die gegevens wel op maar dat betekent niet dat ik het ook ontoegankelijk van anderen moet maken. En hoe vaak dat allemaal netjes gebeurt. Daar zit niet iemand bovenop. Het is niet dat er speciaal op gelet wordt. Tuurlijk kun je gehackt worden, tuurlijk wel, maar er is niet iemand bezig met allemaal monitoren om te zien wat er gebeurde.

I: Want recent zijn we nog een keer gehackt?

R: Ja.

I: En dat zou dus ook bij de gebruikersdata kunnen komen, terwijl wij zeggen dat je zelf mag bepalen met wie je de data wilt delen.

R: Het is onze verantwoordelijkheid om te zeggen 'we delen niet met anderen', dat betekent ook dat je redelijkerwijs moet proberen te beschermen. Natuurlijk kan ik niet weten hoever de FBI zou willen gaan om dat te proberen erbij te kunnen, maar je moet er redelijkerwijs vanuit kunnen gaan dat we niet zullen zeggen welk wachtwoord jij hebt. Qua hobbel zou ik zeggen, dat dit er ook wel een is

I: Jij zegt er zou eigenlijk een iemand verantwoordelijk moeten zijn voor de veiligheid van de data? Zou dat het oplossen?

R: Dat weet ik niet. Er moet in ieder geval specifiek aandacht uitgaan naar dat wij verantwoordelijk zijn voor die data en dat in ieder geval iemand hebt die specifiek hierop let en dat beveiliging gewoon klopt en je kan monitoren dat gebeurt ermee. En of het fout gaat dat we dat meteen door hebben. Vorige keer zijn we erachter gekomen, maar als iemand dat stilletjes had gedaan... Maar daar kan iemand specifiek naar kijken, omdat dat nog wel eens ontbreekt.

I: En je zou natuurlijk ook kunnen zeggen 'daar laat ik een bedrijfje voor langs komen om bij ons in te breken' om te kijken waar de lekken zitten.

R: Ja, dat kan ook, maar dat is een moment opname.

I: Jij wilt eigenlijk dat we daar continu mee bezig zijn?

R: Er moet gewoon iemand naar kijken. Dat hoeft niet gelijk een 40-urige baan te zijn, maar gewoon dat er iemand een taak heeft 'let hierop, kijk hiernaar' en zorg ervoor dat alles netjes...

I: Net als dat DEV4 bijvoorbeeld als taak heeft 'houd de servers draaiend' of dat soort dingen, dat er ook iemand die zegt 'houd de servers veilig', ja.

R: Ja, misschien kun je dan een bedrijf uitnodigen die daar verstand van heeft, weet ik veel, dat zou kunnen, als daar in ieder geval maar aandacht aan besteed wordt.

I: Ok. Heb jij verder zelf nog toevoegingen waarvan je zegt 'misschien kan dat nog helpen met je fantastische onderzoek naar privacy binnen het bedrijf en hoe het naar de buitenwereld gaat?'

[93020301.mov]

I: Zijn er nog dingen die je kwijt wil of zeg je dit is mooi zo

R: nee ik kan niet zeggen volgens mij is het belangrijk de situatie, omdat er gewoon uit onderzoek komt dat mensen die als die een bepaalde situatie doen dan gaan ze een bepaalde handeling ondernemen en karaktereigenschappen zijn heel leuk maar die hebben daar veel minder invloed daarop dan de omgeving.

I: ah

R: Wat dat betreft denk ik dat dat wel aardig is om heel goed kijken naar eh omgeving naar bedrijf Sense want dat geeft een hele grote invloed nog wel meer dan dat mensen gewoon zeggen van oh we willen dit en we willen dat. De grote invloed is gewoon hoe dingen in het bedrijf eraan toe gaan. Daarom zei ik ook screenen van iemand die dat doet eh

I: dat kan

R: dat kan als daar bijvoorbeeld totaal geen controle op zit. Ja dan kan Iemand kan nieuwsgierig worden en gaan kijken weet ik wat weten maakt zijn Ex er gebruik van? Dat zijn van die dingen ja dat zou iedereen kunnen gaan doen in een bepaalde situatie.

[01:08]

I: Ja stel je zou iemand screenen of die wel eens grote hoeveelheden geld heeft gestolen en die heeft zeg maar eh daarvoor een hele tijd van zijn leven in een of ander armoedig dorpje gewoon waar uberhaupt geen geld te vinden was en die gaat vervolgens bij een bank bewerken die zou nog wel in de mogelijkheid zijn om opeens wel eventueel een hele grote hoeveelheid geld eh

R: nee nee ik bedoel iemand die gewoon het idee heeft maar ik vind privacy belangrijk en ik zal het nooit meer doen. zetten we die in de juiste situatie en ik denk dat er een dikke kans is dat hij het nog gaat doen. Dus wat dat betreft,

R: dat dus de situatie heel belangrijk is.

I: Dus je zou hier dan eigenlijk de situatie in het bedrijf zo moeten hebben dat dat gewoon echt not done is om eh

[01:51]

R: ja Een van die dingen is centrale controle en ik denk ook voor andere mensen dat het wel aardig is om naar te kijken is sociale content dat is denk ik de belangrijkste factor die er invloed op heeft op wat er daadwerkelijk gaat gebeuren veel belangrijker dan mensen zeggen dat mensen zeggen dat ze allemaal betrouwbaar zijn

I: Welke dingen zou ik daar voor nog daarbij moeten pakken of zeg je van als je dit in een netwerk neerzet dan komt dat er wel een beetje uit. Mis ik dan nog dingen om die omgeving zeg maar eh in kaart moet brengen?

[02:30]

R: Ja ik weet ik niet hoe je dat precies zou moeten doen. Dat gaat inderdaad dan inderdaad wat eh misschien zelf nu al afschermen van toegang tot die data.

I: ja

R: En dat soort dingen hoe dat geregeld wordt, dat wordt wel vaak gebruikt ofzo. Hoe dat zijn misschien wel van die dingen. ja Ik weet het niet hoe je dat precies zou moeten.

I: nee maar

R: Maar Iets in die richting dat je in ieder geval kijkt gewoon naar wat voor sfeer

I: ja

R: Hoe zit iedereen. Behalve DEV4 en ik, en DEV5 in een hok zetten zeg maar.

I: ja

R: Dat is ook al dat betekent wel dat je het anders doet dat je niet midden door een stapel data heen gaat, als ik hier zou zitten en iedereen tegenover je. Dat zou misschien

I: Dat is waar dat als je inderdaad meer met cubicles zou werken als het ware dan eh

R: ja dat is het allemaal

I: ja nou mooi ik ga het allemaal meenemen. ik denk dat het allemaal wel prima is.

R: hopelijk heb je er wat aan

I: natuurlijk heb ik er wat aan. Het is goed duidelijk in ieder geval

### C.3. Developer 3

[936\_0302].mov

I: kijk wat we vandaag gaan doen is een beetje het netwerk van Sense in kaart brengen en dan vooral van uit jou gezien waar jij mee te maken hebt welke partijen welke mensen welke objecten die met Sense te maken hebben zo software produkten diensten beleidsstukken misschien en dan op basis van dat netwerk gaan we kijken of eigenlijk eerst gaan we kijken van nou wat is jou visie op privacy en hoe past dat binnen dat netwerk zitten daar misschien rare kronkels in waardoor dat netwerk niet op zich zelf stabiel is wat daar verschillende meningen in zitten en daarvoor gaan we eerst het netwerk in kaart brengen en daar hebben we een whiteboard voor

R: ja

#### Network

I: ja dus als jij op het whiteboard zou willen tekenen in het midden een representatie van wat jij bent

R: huh (zucht)

I: je mag zelf verzinnen hoe je eruit ziet. okay En kan jij in de linksboven we gaan ongeveer zes delen gebruiken in de linksbovenhoek wil ik wel graag de drie medewerkers van Sense waar jij het meest mee te maken hebt.

R: moet ik die tekenen of mag ik gewoon eh

I: dat maakt niet heel veel uit

R: okay

I: als je heel graag wilt tekenen dan mag dat

R: en moet ik er nog ruimte tussen laten?

I: nee niet heel veel maar wel een beetje

R: je hoeft geen [onverstaanbaar] te hebben

I: nee die heb ik niet

R: komt wel goed

I: dan heeft DEV2 ze allemaal op gemaakt

R: typisch DEV2

I: ja

R: drie medewerkers van Sense waar ik het meest mee te maken heb

I: ja

R: is dat heel belangrijk

I: je mag er ook vier doen hoor als je daar blijer van wordt hoor maar

R: nee

I: maar je zat te twijfelen tussen

R: DEV2 of STAFF1 of DEV1. Maar ik denk DEV2 eigenlijk uiteindelijk

I: want

R: omdat ik veel met DEV2 te maken heb en maar hij is pas nieuwer

I: en kan je dan rechtsboven de producten of diensten van Sense waar jij mee te maken hebt neerzetten en dat mag zo compleet als dat je het zelf wil

R: CommonSense sense app voor android ehm ja zal ik er maar gewoon 3rd party in, dashboard moet erbij

I: dashboard

R: er veranderd wel veel waar ik mee bezig ben zeg maar het is een moment opname

I: dat is goed ik heb iedereen ongeveer in één week qua interviews dus dan zal moment opname redelijk gelijk zijn. Wat voor 3rd-party dingen heb jij mee te maken inderdaad ja.

R: ehm, ja [schrijft op bord]

I: ja dat is wel heel goed voor het idee. Dan op linksmidden. met welke medewerkers of middelen heb jij of media of pers heb jij te maken voor het naar buiten van Sense

[04:27]

R: nog een keer. met welke medewerkers

I: okay het naar buiten brengen van Sense als in dit is Sense en je hebt de buitenwereld en jij wil Sense de buitenwereld laten weten dit is Sense.

R: eh hm

[05:08]

I: Dat kunnen zijn publicaties ergens, dat kan zijn de website dat soort dingen zeg maar communiceren wat Sense is.

R: En moet ik medewerkers of dingen noemen?

I: allemaal, het mag allemaal. mag door elkaar heen

R: meestal ben ik degene die het zelf naar buiten brengt. iemand

I: dat mag ook.

R: die gesprekken met andere mensen

I: naar wie breng jij het naar buiten dan of wie is jouw publiek

R: mensen die STAFF3 heeft gesproken zo'n beetje.

I: ehm

R: dus ik denk dat STAFF3 het ding is wat eh

I: STAFF3 is het ding. nou dan mag je STAFF3 er neerzetten hoor.

R: ja

I: ja. STAFF3 mag er links bij. Nee hoor STAFF3 is prima als hij in meer hokjes terecht komt

R: lebendrauss [wijst op bord naar waar STAFF3 al staat]

I: Als STAFF3 er op twee plekken staat hebt ik wel door dat dat hetzelfde object is denk ik [06:04]

R: okay en verder developer forum, af en toe een vaktijdschrift. even denken ja ik doe even zo (schrijft nog aanvulling achter STAFF3) demo presentatie, en hogeschool [07:00]

I: En zijn er ook beurzen of bijeenkomsten, waar je.....

R: Ja, maar dat zijn niet echt vaste dingen.

I: Dat zijn echt vaste dingen. (Bevestigend)

I: Maar het is niet echt dat er elk jaar vaste beurzen bezocht worden? Ik bedoel, dat je niet wekelijks naar dezelfde beurs gaat?

R: Er is niet een soort beleid van, we gaan elk jaar naar ICT-delta

I: Ben jij wel degene die daar staat?

R: Ik sta vaak wel op beurzen.

I: Oke. En dan aan de rechterkant, wil ik graag hebben externe bedrijven waar jij mee te maken hebt, dat kan zijn partnerbedrijven, dat kunnen klanten zijn, dat kunnen eindgebruikers zijn. En dat kan dus eventueel via de software waarmee je in aanraking komt. Maar dan wil ik eigenlijk alleen de partijen hebben waarmee je eigenlijk samen wat ontwikkeld, dus als iemand het Sense-platform gebruikt en verder niet met jou in contact komt, dan hoeft die er niet bij, dus alleen partijen waarbij je zelf betrokken bent.

R: Mensen die alleen Sense gebruiken en niet in contact met mij zijn, zijn schaars. Oke, nou als eerste "ask, deal, almende" \*Mompelt\* "LUMC, Parnassia, Hogeschool Rotterdam, ATUS is dus nieuw.."

I: Wat doen die laatste?

R: Beveiliging.

R: We zitten ook in een subsidie project met alle partners, zal ik die gewoon compleet opschrijven?

I: Dat mag.

R: \*Lange denkpauze\*

I: Oke, dan voor linksonder, de vraag eigenlijk, wie zijn de belangrijkste concurrenten voor Sense.

R: Oke, Open-Sense, COSM... \*Denkt\* Er is er nog een... \*Denkt\* Ik denk dat dit de belangrijkste concurrenten van Sense zijn.

I: En wie zijn er, eigenlijk voor het beleid van Sense? Als in, waar gaan we heen met het bedrijf, wat willen we doen? De belangrijkste partij?

R: Intern of extern?

I: Mag allebei. Hij mag bij concurrenten in de buurt, omdat concurrenten bepalen waar je in de markt wel en niet makkelijk in komt.

R: Ik zet het gewoon hier in het midden hoor.

I: Dat mag.

I: STAFF3 staat vaak op veel plekken in het plaatje.

R: Het is best lastig, want eigenlijk is het, wel heel breed.

I: Ja?

R: Volgens mij.

I: Oke.

R: Want ik kan er ook meteen een het UMC en Parnassia tussen zetten want.

I: Omdat je daarmee samenwerkt en dat die dus bepalen wat voor soort opdrachten je doet.

R: Ja, en als het goed gaat met het product dat we daarmee maken, zijn we daarop meer aan het focussen.

I: Ja, dus het is eigenlijk heel erg waar de markt het bedrijf heen trekt, daar gaat het heen.

R: Dat is op dit moment volgens mij wel zo, maar dat noem ik dan STAFF3

I: Ja, dat is goed.

R: En STAFF2 zet ik hier neer.

I: Is STAFF2 daar nog heel erg bij betrokken.

R: Hmm... Ik vind het niet erg direct, nee. Hij heeft wel invloed op STAFF3 natuurlijk, maar dat hebben wij ook.

R: Moet ik Sense erbij zetten?

I: Ja hoor, je mag gewoon Sense erbij zetten, als jij vindt dat iedereen er invloed op heeft, dan kan dat zeker.

R: Dat is een beetje zo.

I: Hoe hebben Google en Apple er..

R: Omdat zij heel erg bepalen wat voor dingen er met smartphones kunnen. En, daar zijn wij toch een beetje ervarener in.

I: Dus het is meer wat voor platform zij bieden..

R: Ook als zij zeg maar functionaliteit van Sense gaan overnemen, dan moeten we daar ook rekening mee houden.

I: Oke. Zijn er nog wetgevende partijen, zeg maar, belangrijke dingen waar je dan rekening mee moet houden? Wetten, regels?

R: Ik denk dat als je je beleid helemaal vanaf het begin laat sturen door wetten en regels, dan gaat het heel langzaam.

I: Ja. Dus die wetten en regels zijn dus nu niet de belangrijkste..

I: Dan een vraag, is er eigenlijk een beleid van Sense ergens vastgesteld of, is er een beleid of een strategie van waar zijn we over vijf jaar?

R: Niet dat ik weet. Er is in ieder geval geen overleg over gepleegd.

I: Oke. Dus dan, als er zeg maar die bedrijven bepalend zullen zijn voor het beleid, dan zou jij het ook moeten weten op het moment dat er zoiets zou komen? In de ideale wereld.

R: Ja, maar het beleid wat er nu ligt, is nogal ad hoc. Dus een jaar vooruit. Jij vroeg, is er een beleid vanwaar Sense ligt over vijf jaar, ik denk dat iedereen daar wel een beetje een idee over heeft maar het is nooit echt...

I: Het is niet van we werken met die en die bedrijven samen en..nee?

R: Nee.

I: En waar zijn we over één jaar dan? Jij zegt het is meestal een jaar vooruit, is dat vastgelegd of?

R: Volgens mij is daar niet een document van, nee.

I: Oke. En hoe komt dat bij medewerkers terecht, het idee van wat doen we?

R: Dat komt uit de medewerkers zelf een beetje. En vooral STAFF3, van wat gaan we doen met deze partij. Iedereen is zo vrij om aan zijn eigen project te klussen. Ik denk dat dat deels uit de medewerkers zelf komt en een deels uit STAFF3.

I: Laatste vraag voor het netwerk, zeg maar de minder op platform producten gaan we ontwikkelen en meer op de visie van het bedrijf. Wie zijn daar bepalend voor? Dat is net weer even anders als van waar moet je in de markt zitten, maar meer wat willen wij, voor wie zijn wij, wie bepalen het?

R: Nieuw lijstje?

I: Dat mag een nieuw lijstje zijn.

R: Volgens mij is dat Sense, eigenlijk.

I: Dat is goed hoor. Zit STAFF2 daar wel of niet bij?

R: Nee, die zit daar niet bij, ik denk het niet.

I: Of is dat misschien een overgang, dat STAFF2 daar eerst bij zat, en nu niet?

R: Ja, hij heeft Sense de goede kant op gestuurd, heel erg. Toen was STAFF2 de enige die bepaalde hoe Sense heette en waar we mee samenwerkte. Maar sinds wij hier zitten, komt hij



hier kijken om te kijken waar wij zijn en zegt het zal mij leuk lijken om..

I: Dat is dan al minder sturend dan het voor hem was?

R: Ja.

I: Dus nu heeft STAFF3 eigenlijk meer die rol?

I: Dat waren de vragen voor het maken van het netwerk.

## Privacy

I: Dan, komt nu vraag, wat is volgens jou privacy?

R: Privacy is de controle die je hebt over welke informatie over jezelf beschikbaar is aan elk ander mens.

I: Oke. En hoe uit zich dat in datgene wat er bij Sense gebeurt, de software die ontwikkeld wordt, de producten, diensten? Hoe zie jij zeg maar privacy in de wereld van ubiquitous Computing.

R: Bij Sense is het nu een beetje ingewikkeld, we doen twee dingen, we hebben ons eigen Sense platform waarbij je om te beginnen alleen jezelf toegang geeft tot informatie die je zelf over jezelf verzameld. En het idee is om dat je dat dan ook aan andere mensen beschikbaar te kunnen maken. Aan de andere kant zijn er van die 3rd party dingen, die zijn gemaakt zodat iedereen die erbij komt automatisch status-informatie met het systeem deelt en met de globale meester-administrator. Dus in eerste geval hoe zie ik privacy in Sense of?

I: Hoe zie jij privacy naar voren komen in wat Sense doet?

R: In eerste geval is privacy heel erg ingebakken, tot op het vervelende af zo'n beetje. In tweede geval is privacy een beetje impliciet en moet je maar hopen dat de eindgebruiker er op een goede manier mee omgaat.

I: Dan krijg je een soort centralist, die alle data van iedereen kan overzien

R: Het is geen evil empire, maar wel met bijvoorbeeld voor alle deal gebruikers is er een account die van alle gebruikers kan zien waar een autotje gereden heeft. Dus het is niet heel erg wat er gebeurt, maar het is niet heel erg transparant.

I: Wordt die data niet gedeeld met wie je gebeld hebt? Maar wel naar de server geupload door de app die die drivers..

R: In sommige gevallen verzamelen we iets meer data dan dat we delen met iedereen, ook bijvoorbeeld met iVitality, Daar hebben we een slaapsensor, die maakt gebruik van geluid, beweging en licht dus die verzameld data over het net. En die slaapdata wordt dan gedeeld met SSCH Maar dat soort dingen zijn dus niet heel duidelijk gecommuniceerd naar mij en cliënten.

I: Dus voor jou zou dat transparanter kunnen? Je wil controle hebben over welke informatie beschikbaar is over jou. Zit daarin ook dat stukje dat je...

R: Het zou het mooiste zijn als je het vinkje hebt deze app gaat deze informatie van jou delen met deze mensen. Dat is de ideale privacy voor mij. Als je bijvoorbeeld een app van de appstore haalt dan zegt ie dit gaat voor speciale permissies vragen, dat zou je ook kunnen doen met je sensordata.

I: En omdat het platform natuurlijk vrij generiek is heb je soms ook meerdere partijen die bij je data zouden willen, toch? Hoe zou je dat voor je zien om daar een transparant overzicht in de kunnen houden?

R: Ik denk aan bijvoorbeeld Facebook, daar heb je een lijstje met apps, dat is een lijstje die naar jou persoonlijke gegevens kunnen, die je geboortedatum, naam en vrienden kunnen zien.

I: Hoe, denk je bijvoorbeeld over, als je data deelt met zo'n app, en die app zou het bijvoorbeeld voor weer andere doeleinden gebruiken, dan wat zij alleen maar zeggen, valt dat ook onder het stukje privacy wat jij ook als Sense geeft?

R: Daar heeft Sense niets mee te maken, als jij besluit om je data aan iemand te geven dan is het je eigen verantwoordelijkheid dat die gene ermee goede dingen mee doet

I: Als jij dus je data upload naar CommonSense dan vertrouw jij als gebruiker daarop dat Sense dat niet zomaar aan andere partijen afstaat, toch?

R: Ja.

I: Oke, zou jij dan ook qua transparantie willen kunnen zien wie op dat moment jouw data heeft gebruikt of ingezien?

R: Ja, het zou leuk zijn, maar niet heel erg belangrijk.

I: Jij hebt een verbinding met die persoon en jij zegt die persoon mag deze gegevens van mij.

R: Tuurlijk is het dan extra netjes als je ook kan controleren wat iemand heeft gezien, maar dat is niet een vereiste.

I: Nu heb ik, een paar mensen al gehoord over bijvoorbeeld beveiliging van data, hoe denk jij daarover, wordt dat genoeg gedaan is dat.. hoever moet je daar in gaan, is het überhaupt nodig?

R: Dat is wel nodig volgens mij, op dit moment wordt het niet genoeg gedaan. Het minste wat ik graag zou willen hebben, als iemand toegang tot de server krijgt alsnog bij de data die in de database staat kan komen.

I: Op dit moment, als jij medewerker van Sense bent, kan jij in principe bij de data die gebruikers uploaden naar de server?

R: Ja. Niet iedere medewerker kan dat, maar ik wel.

I: Is dat een probleem of tegenstrijdig met hoe jullie de privacy zien?

R: Natuurlijk. Maar, er staat tegenover dat de gebruikers nu op Sense zitten, weten dat het een testfase/beta is die nog niet helemaal is ontwikkeld.

I: Maar als het minder beta zou worden zou dat wel nut hebben?

R: Medewerkers van Sense zouden wel bij de data moeten kunnen. Dat is eigenlijk wat wij doen. Ik denk dat een medewerker mag zien wat de hoeveelheid data is, wanneer was de laatste activiteit.

I: Hoe denk jij dat de andere partijen in dit netwerk over privacy denken? Bijvoorbeeld de resterende partijen? Komt dat redelijk overeen met wat jij zou willen?

R: Dat wisselt een beetje bij de partijen. Waarbij sommige partijen geïnteresseerd zijn door het verzamelen van data bij hun gebruikers. Maar, ze willen daarbij wel gebruik maken van wat er verzameld wordt. Dus eigenlijk denk ik dat we het allemaal wel een beetje eens zijn.

I: Maar dat sommige partijen data aggregeren, dat een middel is..

R: Ja, maar iedereen beseft wel tegenwoordig dat je niet een klant kan hebben die data van mensen jat. Anders ga je niet met Sense door de deuropening, denk ik.

I: Hoe denk je dat bijvoorbeeld de twee concurrenten, gaan die anders om met privacy dan Sense doet, of jij vindt dat...?

R: Weet ik eigenlijk niet, volgens mij hebben we redelijk hetzelfde model.

I: In de communicatie naar buiten toe, dus bemiddelings..dingen.. komt privacy daar vaak naar voren?

R: Ja, best wel. Veel mensen hebben als eerste reactie.. ooooh. Het komt wel als eerste als gesprekstof naar voren. Maar we hebben het er zelf meestal niet over, meestal andere mensen.

I: En als je bijvoorbeeld met zo'n third-party een app ontwikkeld, gaat het er dan wel eens over?

R: Ja, dan gaat het er vrij snel over, omdat privacy dingen wel ingewikkeld maakt.

I: Zien ze het dan vaak als een probleem, dat er rekening mee gehouden moet worden?

R: Nou ja, het is een probleem maar ook onderdeel van. Dus ja, een probleem maar niet dat ze het uit de weg willen hebben.

I: Maar dat is ook niet wat zij willen?

R: Nee.

I: Qua functionaliteiten in de software, die we hebben als Sense, hoe zit het daar met de elementen van privacy, gaat het daar goed mee? Voldoet dat aan jouw wensen?

R: Producten die wij nu maken?

I: Die je nu maakt.

R: Bijna. In common sense, voldoet het strikt genomen wel aan de definitie, maar het is zo ingewikkeld dat het wel beter kan. Transparantie

I: En de Sense-App?

R: Die zie ik als onderdeel van CommonSense

I: En dashboard dan ook?

R: Bij dashboard? Is een stap vooruit gedaan denk ik, ja.

I: Oke.

R: Want daar heb je op het moment dat je een widget toevoegd waarmee je mensen toestemming geeft tot je data, dan geef je deze mensen toestemming om je data te zien en hoelang? En die toestemming kan je ook weer intrekken. Dat is een stapje in de goede richting.

I: En zijn er dan plannen om bijvoorbeeld CommonSense naar die richting te trekken van de goede richting, een stap in de goede richting? Of is dat niet nodig omdat dashboard het nieuwe ding is onder gebruikers?

R: Ik denk.. daar is niet echt over nagedacht. Het is een beetje raar. Maar er zijn überhaupt geen plannen om iets met CommonSense te doen, er is geen tijd om er iets mee te doen.

I: Oke.

R: Het is niet zo dat we niets aan Common Sense willen doen, maar er zijn gewoon geen plannen voor.

I: Want de plannen die er zijn, zijn er voor het ontwikkelen van 3rd party apps?

R: Ja, en CommonSense moet ik gewoon in mijn vrije tijd doen

I: Want in de third-party apps, daar zitten de budgeten.

R: Daar komt nu het geld vandaan. En ja, we zitten gewoon krap in de uren die mensen hebben.

I: Oh.

R: Het is niet door onwil, dat de beveiliging slecht is, of dat we terroristen in onze privacy uitvoering willen, maar door onkunde.

I: Want er zijn niet meer uren in de week, en niet meer werkuren in de week.

R: Precies.

I: Als mensen op een gegeven moment hun toestemming voor het delen van data met bepaalde mensen-partijen willen stoppen, kan dat? En is dat makkelijk te doen, of is dat het proces is erg complex en moeilijk.

R: Ja, precies dat. In iVitality hebben we daar een scriptje voor gemaakt, maar dat moet je maar net vinden. En voor CommonSense moet je maar gewoon een mailtje sturen.

I: Oke en zeggen, ik wil mijn data kwijt?

R: Ja. Het kan zeker, maar het kan zeker beter. En in Dashboard is daar een slag in de goede richting gedaan.

I: Oke. Hoe komt het dat dashboard – het is natuurlijk nieuwer - maar er zijn ook inzichten gekomen dat..

R: Dashboard is iets wat wij helemaal zelf hebben gebouwd en daarbij is managen van privacy een belangrijke feature. Want als we Sense een keertje aan de mensen beschikbaar willen maken, moeten we de privacy goed hebben.

I: Maar die partijen waarmee jullie al samenwerkten, daar ontwikkel je samen mee, dus die hebben er minder last van dat het binnen Sense nu nog niet helemaal is zoals je het zou willen qua privacy?

R: Dat denk ik wel, dat je daar impliciet daar al..de gebruiker weet al, ik doe dit omdat ze dan bij het LUMC kunnen zien hoe het met mij gaat. Dus die hebben daar al een impliciete regeling voor. Terwijl Sense, daar download je en ga je mee aan de slag. Als het dan duidelijk is dat er iets gebeurt.

I: In de communicatie van de apps en toepassingen die je van de website kan vinden of de app-store is het daar duidelijk wat er gebeurt met de data?

R: Ik weet alleen van Sense-app in Android dat je uitleg krijgt wat is de Sense app. Wat doen jullie met de data en van wie de data is. Hoe het precies gaat met toegang geven aan anderen, moet je iemand hebben van Sense. Dus het begint zeg maar meer complexer.

I: Maar wat er dan dus staat in app stores, is eigenlijk de data is van jou, en jij bepaald wat je ermee doet. En verder kan er niemand bij, maar eigenlijk kunnen er een aantal mensen van Sense wel bij. Zit dat ook een beetje scheef dan? Is dat een probleem? Of wij zijn het bedrijf dat het ontwikkeld dus logisch dat dat kan.

R: Nee, het is niet de bedoeling dat dat zo is. Ja, daar heb je gelijk in.

I: Ik weet niet hoe dat bij anderen bedrijven is, of het gebruikelijk is of je wel of niet bij de data moet kunnen.

R: Nu werk je in een soort groter cloud ding, je leent een stukje common sense, daar is het meestal dat je geen toegang hebt tot wat dan ook van je gebruikers.

I: Dus omdat er zoveel gebruikers zijn, is het niet meer te doen..

R: Nou ja, bij Sense is dat ook eigenlijk niet, tenzij je echt in de SQL gaat kijken.

I: Hoe zou dat bij Google zijn, kunnen zij als ze zouden willen, al je data zelf bekijken?

R: Als ze willen zouden ze vast allerlei data kunnen bekijken.

I: Bij OpenSense of bij Cosm?

R: Ik ga ervanuit dat ze hetzelfde beleid hebben als wij. En ik ga ervanuit dat ze wat verder zijn dan wij.

I: Wat maakt Sense ten opzichte van die twee uniek? Wat is er anders?

R: Meer features. Onze sensoren.

I: De dataverwerking?

R: Ja, dat is het inderdaad. Want bij anderen kan je een beetje visualiseren en werkbaar maken. Een beetje wat er bij Sense ook kan.

## Covenant

I: Stel je voor jij zou Sense zijn, wat zou jij aan de wereld willen beloven ten opzichte van privacy?

R: Mijn definitie van privacy.

I: Controle over welke info je wilt delen.

R: Ja, en het liefst iets sterker, als er iemand per ongeluk toch bij de data van Sense kan komen, dat die alsnog er niets mee kan. Dus, dat iemand van Sense niet kan inloggen en erbij kan. Of iemand van externe partijen zoals de beveiliging.

I: Wat zou er binnen dit netwerk moeten gebeuren om te zorgen dat jij die belofte waar zou kunnen maken? Wat zijn de belangrijkste dingen? Bijvoorbeeld een bepaalde hoek van de markt waar je wel of niet heen moet.

R: Volgens mij heeft dat niets met het netwerk te maken. We verkopen Sense ook op dit moment, zonder het schenden van privacy. Ook al zouden we de privacy kunnen schenden.

I: De belofte klopt dus wel ongeveer, alleen communiceer je iets, wat je niet helemaal waar kunt maken.

I: Dus wat er eigenlijk zou moeten gebeuren dat wat je communiceert waar is. Het makkelijkst zou dan zijn, dan zeggen we niet dat het zo is. Maar dat is niet wat je wil, neem ik aan?

R: Nee.

I: Want je wil dit wel kunnen beloven, dus dan is er eigenlijk wat zou moeten gebeuren, is aanpassing in de software.

R: Zoals het bij Sense een beetje gaat, eerst zeggen dat we het kunnen, en het dan pas maken. Zo is dat nu ook met privacy. Net als bij een iPhone app, is er heel lang gezegd: tuurlijk we doen ook iPhone, en op een gegeven moment heeft DEV2 het maar gemaakt. Of een OBD-II sensor, om maar een ander groot probleem te noemen.

I: Volgens mij heb ik mijn vragen wel gehad Jij nog dingen die je wil toevoegen?

R: Nee, niet echt, denk ik. Wat ook wel interessant is, is om te kijken naar hoe het in de apps zelf allemaal geregeld is, want een app zelf is ook een soort entry-point.

I: Ik ga er nu vanuit dat jij weet hoe het in de Sense app geregeld is, of is dat naïef?

R: Ja, nou ja, ik krijg zo een lijst van alle features van wat we uitlezen uit de telefoon, en dat doen wij ook allemaal, en sturen door naar CommonSense. maar de vraag is of andere apps of Google kunnen zien wat er verzameld wordt. Het is niet de bedoeling, maar wellicht dat dat zomaar zou kunnen. Ik bedacht me gewoon, ik kijk alleen maar naar CommonSense, en niet zo zeer naar de apps.

I: Maar dat zou dus ook gelden voor third-party apps, maar dan alleen het stukje Sense, function-aliteit. Zeg maar de package..Sense iets..

R: Het is allemaal zo gemaakt dat er geen andere apps bij kunnen maar, het is nooit echt heel erg een beleid over geweest. Nee, dat is niet waar. Het was altijd zo dat Sense een platform was waar andere apps tegenaan konden praten, maar dat werkt gewoon niet. Dat maakt het ook gewoon ingewikkeld om te controleren wat er gebeurt. Dus vandaar dat we er af zijn. Dat is niet allemaal zo heel erg relevant.

I: We hebben nu natuurlijk ook genoeg antwoorden.

## C.4. Developer 4

[936\_0297].mov I: Nu moet ik natuurlijk eerst vertellen wat we gaan doen vandaag.

R: Ja

I: Ik ga je zo wat vragen stellen over met welke mensen, producten en omgevingsdingen je te maken hebt binnen Sense. Vervolgens gaan we kijken naar het onderwerp privacy data, informatie privacy en hoe jij daar over denkt en hoe jij vindt dat Sense daar over moet denken of denkt. En hoe dat in je hele netwerk terugkomt en vervolgens kijken we of dat dan rare situaties geeft in jouw netwerk bijvoorbeeld.

R: Ja

I: Is dat tot zover duidelijk?

R: Ik denk het wel. Als het mooie gestructureerde kleine vragen zijn.  
I: Ja dat zijn hele mooie hele kleine vragen. Wil jij het liefst op een white board tekenen of wil je het liefst op papier dingen uit tekenen wanneer ik zeg dat we een netwerk gaan tekenen.  
R: Ik denk op papier  
I: Gelukkig hebben we papier  
R: Is dat ook al een puntje voor privacy testing

## Network

I: Nee hoor. En je mag kiezen welke dingen je wilt nemen. De eerste vraag: kun jij een soort poppetje of een stip in het midden tekenen?  
R: Ok.  
I: En dat stel je dan zelf voor. Kan jij daarbij tekenen met welke mensen van Sense jij het meest te maken hebt.  
R: Welke mensen ik het meeste te maken heb? In de vorm van namen?  
I: Ja daar mag ook een poppetje bij getekend als je wilt hoor.  
R: tekent?  
I: Een stip en naam ofziets  
R: nog een afstand of een dikte van een lijn die aangeeft van hoe de correlatie is? waar ik het meest mee te maken heb?  
I: Als je dat wilt. dat mag maar het hoeft niet  
R: maar het moet een keer?  
I: nee, je mag meerdere mensen neerzetten  
R: Oke directe relatie tja. [stilte tijdens opschrijven]  
I: ja? Zijn dat ze?  
R: Ik kan iedereen er wel bij bijzetten  
I: Ja je kan iedereen er wel bij zetten maar. Dit zijn de mensen waar je het meeste mee te maken hebt zeg maar.. Qua werk enzo.  
R: Ja de meesten. Als je er een gouden top drie bij moet halen dan is dit het als ik het op moet schrijven.  
I: Met welke producten van Sense heb jij te maken?  
R: Welke producten ik het meest mee te maken heb? En dan welke software tools ik gebruik gedurende mijn werk?  
I: Nee, welke Sense producten  
R: Wat is een sense product? We hebben zoiets als backend, commense, data opslag...  
I: Je mag het op schrijven als backend  
R: PHPAPI, MYSQL mongodb, backend dan heb je nog data processing. De ene kant opslag, de andere kant data. Beiden online.  
I: En front-end toepassing zoals apps enz.  
R: Ja  
I: Met welke mensen heb jij het meest te maken als het gaat om het naar buiten communiceren van wat Sense doet en wat Sense is en wat voor producten er zijn? Is dat bijvoorbeeld met STAFF4 of direct met pers mensen of met STAFF3, als zijnde de persoon die met de buitenwereld communiceert? Kortom, hoe communiceert Sense naar de buitenwereld?  
R: Ik begin mij af te vragen of ik met de buitenwereld communiceer. Redelijk direct met de mensen die ik spreek, denk ik. Het is niet dat ik een bepaald kanaal gebruik om dingen aan de buitenwereld bekend te maken. Een klein deel door STAFF3, die komt bij de klant om nieuwe mensen aan te trekken dus als er nieuwe features zijn dan via STAFF3.  
I: Je zei dat je het redelijk direct doet, naar wie?  
R: Naar iedereen die ik spreek.  
I: Als ze vragen naar je werk?  
R: Ja, maar niet direct met als doel ze te informeren, maar wanneer ze ernaar vragen.  
I: Maar nooit pers of iets dergelijks? Misschien ga je wel eens naar evenementen waar Sense staat?  
R: Ja, wel eens geweest ja.  
I: Wat voor evenementen zijn dat? Zou je die organisaties erbij willen schrijven?  
R: Dan hebben we het over 'naar buiten toe'?

I: Inderdaad. [Schrijft organisatie bij op papier]

R: Zoiets.

I: En daar hang jij dan op de een of andere manier aan vast?

R: Ja. En dan natuurlijk nog meetings en onderzoek.

I: DevLab is een partnerbedrijf. Zijn er meer van dat soort bedrijven?

R: Buiten DevLab om?

I: Inderdaad. Vanuit Sense gezien.

R: Ja, niet echt partnerbedrijven, maar bedrijven waar ik nu regelmatig kom, vanuit waar ik zit natuurlijk. Maar niet om te communiceren wat er intern allemaal gebeurt.

I: Werk je daarmee samen?

R: Nee. Dat was eigenlijk het idee, maar dat is nog niet van de grond gekomen. Er is nog geen samenwerking. Al met al, er is niet een specifieke samenwerking te noemen met een groot bedrijf, maar een aantal kleine communicaties met kleine bedrijfjes.

I: Zijn er ook bedrijven of mensen aan te wijzen als zijnde klanten of een product of service-app? Of heb je daar niet heel veel mee te maken?

[10:20]

R: Nee, ik heb daar niet veel mee te maken. Als ik kijk naar de laatste bijeenkomst en gesprekken die ik gehad heb niet. Van de week TNO, maar dat was meer partnering. Het zoeken naar een afstudeerder voor beide partijen. Dan kijk je naar de faciliteiten die Sense heeft, wat zij doen en hoe je dat kunt combineren. Maar niet klantgericht. Het is samenwerking, maar niet met grote spelers. De week ervoor een netwerkbijeenkomst waarbij mensen die met sensor data bezig zijn spreekt in kleine groepjes, maar ook dit zijn geen klanten.

I: Kom je daar vaker op die meetings?

R: Zal ik hem intekenen?

I: Ja doe maar. Echte eindgebruikers zul jij dan ook minder mee te maken hebben?

R: Ja. Eindgebruikers? Ja, omdat ik mij wel regelmatig met PHPAPI bezig houd, waar veel developers op zitten. Maar zijn dit eindgebruikers?

I: Het zijn partijen waar je mee te maken hebt. Ga je om met developers buiten Sense? Ben je daar het aanspreekpunt voor?

R: Nee, ik ben daar niet het aanspreekpunt voor. Ik weet ook niet wie het aanspreekpunt is, maar ik heb heel veel bijvoorbeeld in chats staan en omdat het heel vaak via-via bij mij terecht komt, wordt het ook vaak direct gedaan. Ja, er wordt veel gecommuniceerd over functionaliteit met developers en buitenstaanders. [Schrijft bij op papier]

I: Bij zo'n netwerkmeeing zeg je dat er andere partijen bezig zijn. Zijn dat concurrenten van Sense? Of beter, zijn er concurrenten van Sense en zo ja, welke dan?

R: Nee, niet echt bedrijven die precies hetzelfde doen. Het is meer een grote gesubsidieerde infrastructuur waar meerdere bedrijfjes gebruik van maken. Het is eigenlijk meer voor partnering. Maar daar zullen misschien kleine bedrijfjes tussen zitten die concurrent zijn.

I: Zijn er in het algemeen bedrijfjes aan te wijzen die hetzelfde doen als Sense? Of vergelijkbare dingen waardoor ze als concurrent te zien zijn?

R: Ja, op kleinere vlakken. Die zijn er. Bijvoorbeeld TNO, waar ik geweest ben, TNO is eigenlijk een heel ander soort bedrijf, die zijn meer onderzoekgericht. Ze zijn niet direct concurrent maar doen wel gelijksoortige dingen. Een bedrijf waar we in Assen een keer geweest zijn, dysi heette dat volgens mij.

I: Zou je dat bedrijf erbij kunnen zetten?

R: [schrijft bij]

I: En verder nog?

R: Qua concurrenten? Waar ik contact mee heb?

I: Waarvan je weet dat ze bestaan.

R: Google.

I: Google?

R: Die gaat uiteindelijk hetzelfde doen wat Sense doet. Data verzamelen en tracken van gebruikers om bepaalde informatie te geven. Dus ja, dat is een redelijk grote concurrent. Die doen hetzelfde als Sense.

I: Maar waarom zijn ze anders? Of zijn ze niet anders?

R: Ze doen minder patroonherkenning. Het is meer sensordata opslag om stromen makkelijker

te krijgen en zodat je daar weer wat mee kan doen. En Sense doet dan ongeveer dit stukje wat ernaast staat. En wat dat betreft zijn ze gelijk en in dit stukje zijn ze anders.

I: Sense doet meer met dataprocessing?

R: Ja en bij Dysi gaat het meer om dataprocessing en gaat het weer niet op –opslag. Ze focussen zich op maatwerk voor klanten, maar dan richten ze zich niet op wat ze in eigen instantie hebben zoals patroonherkenning. Patroonherkenning is meer wat wij weer doen. De toepassing die ze gaan leveren aan klanten zal ongeveer gelijk zijn. Maar wat wij bieden is dat het in de cloud is en dat wij het lekker generiek kunnen houden. Google heeft alles.

I: Ok. Wie bepalen er eigenlijk binnen het bedrijf – binnen Sense – welke kant erop gegaan wordt?

R: Beginnen we dan bij het begin?

I: Misschien een rare vraag om hier te stellen.

R: Je mag er ook op terug komen op een ander tijdstip?

I: Nee, we slaan nu een aantal vragen over die we al behandeld hebben. Beleidsmakers?

R: Als je kijkt naar het begin, want Sense is nog niet zo heel oud, met stip is dat STAFF2. Moet ik die nog ergens tekenen?

I: Ja, je mag STAFF2 ook ergens tekenen. Maar is STAFF2 nog van Sense?

R: Nee, hij staat waarschijnlijk niet op de loonlijst, maar is eigenlijk de 'baas' van Sense. Hij is eigenlijk de gene die bepaald welke kant erop gegaan wordt.

I: Dus hij mag eigenlijk ook op de lijst gezet worden. Of hang hem ergens aanvast op het randje.

R: [schrijft] In eerste instantie STAFF2 dus eigenlijk, die bepaalt de richting in grote lijnen, maar soms ook heel duidelijk 'dit willen we hebben, dit is Sense'. Daarna STAFF3, maar ook weer wat grote lijnen. Daarbinnen hebben wij zelf natuurlijk een grote invloed hoe het eruit ziet, maar ik denk STAFF3.

I: Ok.

R: Moet ik het nog kleurtjes geven?

I: Nee, dit komt wel goed. Als je graag wilt heb ik hier een marker, dan mag je STAFF2 een kleurtje geven.

R: [geeft kleurtje]

I: Ok. Zijn er nog wetten of regels, mensen of instanties, waar je vanuit Sense mee te maken hebt? Die misschien van invloed kunnen zijn op het beleid?

R: Dat is breed.

I: Zijn er wetgevende machten die beïnvloeden waar Sense heen kan in de markt?

R: Poeh. Trickey. Waar Sense heen kan [denkt] Weet ik niet. Ik denk niet dat die heel sturend zijn.

[20:00]

I: En even weer terug naar de mensen die het beleid maken? Bepalen die ook de visie, alsin "wat is Sense"?

R: Ja, in grote lijnen. Het is niet zo dat het een alleenhanger is. Het is meer, in een bepaalde volgorde, wie er het beleid en visie maakt. Maar dat zegt niet dat wij geen visie hebben.

## Privacy

I: We gaan het hebben over visie. Of eigenlijk over privacy. Dan wil ik vooral van jou weten wat privacy is met betrekking tot dataverzameling. Dus, met betrekking tot wat Sense eigenlijk doet. Wat is jouw visie met betrekking tot privacy en ubiquitous computing?

R: Mij visie op Privacy.

I: Of wat is privacy volgens jou?

R: Privacy is dat gebruikers die onze platformen gebruiken de enige zijn die recht en mogelijkheden hebben tot hun data. Zij zijn de enige die het kunnen zien. En zij zullen altijd de eigenaar blijven. Dat vind ik privacy. Dus ja, geen mogelijkheid dat data ter beschikking gesteld wordt, zonder dat zij het weten. Dus geen kleine lettertjes waarin je zegt dat het stiekem verspreid kan worden. Dus gewoon heel transparant zijn naar mensen, van 'he, dit is er aan de hand'. Dat je transparant bent en mensen duidelijk maakt wat de gevolgen zijn. Dat hangt er mee samen.

I: De partijen die je hebt getekend. Hoe denken die over privacy? Of zijn er partijen die er erg uitspringen die precies hetzelfde of juist heel wat anders denken?

R: Ik heb eigenlijk geen idee hoe die over privacy denken. Maar volgensmij is het common sense. Het is niet de bedoeling dat je een gratis account hebt waarmee data voor iedereen

beschikbaar is. Niet iets als facebook. Ze bieden een service aan, maar ondertussen is het twijfelachtig hoe privacygevoelig data is. Maar voorzover ik gezien heb, is dat hier niet het geval. Bij Google denk ik hetzelfde, hoewel er services zijn waar gebruik gemaakt wordt van je data en je je data ter beschikking stelt. Als we teruggaan naar wat wij aanbieden en wat zij aanbieden, database, data verzamelen en data analyse eroverheen gooien, dezelfde services, is dat ook gewoon afgeschermd. Het is niet zo dat die data eenvoudig bereikbaar is. Ik denk dat zij ook ongeveer hetzelfde met privacy hebben en dat ze daar veel voor doen. Maar ik denk dat ook, omdat ze wel een beetje terughoudend zijn met de clouds. Ze willen niet zozeer hun spul online hebben. De bedrijven waarvoor ze werken hebben ook wel gevoelige data hebben waarop ze analyses doen. Daarom willen ze data vaak afgeschermd hebben of niet buiten een bepaald gebied hebben. Dus die hebben privacy ook wel aardig hoog in het vaandel staan.

I: En dan ook op dezelfde manier zoals jij net beschrijft? Dat de data altijd van de gebruiker blijft en dat de gebruiker het altijd zal moeten kunnen...

R: Ja, ik denk het wel. Ze doen voor specifieke partners projecten en verzamelen niet zoveel mogelijk data waarop ze misschien nog wel analyses kunnen doen.

I: Hoe zit dat bij Sense? In de producten?

R: Hoe ik beschreef zoals het zou moeten zijn of hoe het daadwerkelijk is? Het is zo dat gebruikers recht hebben over hun eigen data. Alle data wat ze uploaden kunnen zij bij en alleen zij bepalen wat er gedeeld wordt. In dat opzicht denk ik dat het zo is, zoals we willen. We kunnen niet zomaar allemaal data voor analyses gebruiken om meer informatie te verkrijgen.

I: Dus, stel ik zou erbij willen kunnen, bij die data, dan zou dat niet lukken?

R: Als wie?

I: Als admin?

R: Dat is een ander puntje. Als admin kan dat wel. Ik ken geen partij die dat niet zo heeft. Je hebt bepaalde levels van security en privacy: hoe makkelijk kun je erbij komen? Als admin kun je erbij en kun je bij data van anderen.

I: Je bent nog steeds geen derde partij.

R: Nee, precies. Je doet zaken met ons en je moet ons als Sense vertrouwen. Dat is spannend voor de overheid misschien. Mensen die bij de balie werken kunnen de gegevens weer inzien. Het is niet zo dat het op straat komt te liggen.

I: Nee, nee, nee. Ziet die gebruiker dat? Wanneer er iemand van Sense naar je data gekeken heeft.

R: Nee, dat ziet hij niet.

I: Stel je zou gebruikersdata veranderen. Zou de gebruiker dat dan zien?

R: Misschien moeten ze dan een eigen administratie ernaast hebben, maar nee, ze kunnen dat niet zien.

I: De data die verzameld wordt, dat is in principe wat de gebruiker zelf wil wat er verzameld wordt? [30:00]

R: Ja, volgensmij is dat redelijk transparant. Volgensmij staan er in alle apps settings wel alle vinkjes van data die je wilt dat er verzameld wordt. Ik denk dat je er van op de hoogte bent dat alle telefoonnummers die je gebruikt ook verzameld worden, maar dat weet ik niet zeker. Dus, hoe duidelijk het is wat er verstuurd wordt, hoe duidelijk het naar buiten gebracht wordt, weet ik eigenlijk niet. Ik weet niet zeker of dat wel duidelijk genoeg is en of alles er wel in staat. In de code staat ook per "vriendje" – zoals dat op facebook genoemd wordt – wat er verstuurd wordt, dus misschien weet men niet wat er allemaal verstuurd wordt.

I: Van dat rijtje partijen dat hier staat en het denken over privacy, komt dat ook overeen met wat Sense – of wat jij – vindt?

R: Of zij ook op dezelfde manier met privacy omgaan?

I: Ja

R: Even kijken, dat denk ik wel ja. Dat is heel lastig te zeggen van third party developers. Het is een brede groep, iedereen die kan connecten met onze API en iedereen kan er programma's bovenop gooien. Je gaat naar onze website, claimt iets te doen, gebruikt data van onze database en ja, je weet niet wat ze ermee doen. Of ze dingen schenden. Dus dat kan ik niet zeggen. De manier waarop ze met Sense communiceren is het wel zo dat mensen zelf toestemming geven dat een third party van de database gebruik kan maken. Het is niet zo dat ze zomaar in de database kunnen rondlopen. Ik weet zelf ook niet hoe deze instanties daar instaan, ik denk niet dat wij een



heel andere gedachte over privacy hebben.

I: Denk je dat die andere partijen ook duidelijk genoeg hebben hoe Sense vindt dat er met gebruikersdata om gegaan moet worden?

R: [Denkt na] Ik denk niet alle partijen. Het is niet dat met het ene contact evengoed contact is als met andere partijen. Het is wel vaak zo dat mensen vaak beginnen met "O, Big Brother" en dan hebben ze het idee dat het een monitoring systeem is dat helemaal niet voor de gebruiker ten goede komt, maar voor iets anders ofzo. Dus van "O, gevaarlijk, Big Brother", want het kan gebruikt worden voor andere doeleinden. Ik denk dat partijen die buiten Sense staan dat als eerste idee hebben en dat ze het idee hebben dat Sense andere dingen doet met de data. Partijen gelinkt aan Almende zullen het wel doorhebben, want daar zit ook onze externe communicatiemedwerke

I: Ask, Deal, DO.

I: En daar hangt STAFF2 natuurlijk ook weer aan vast.

R: Of zij er ook hetzelfde over denken, of ze weten hoe zij dat doen. Ik denk wel dat zij dat weten.

I: Denk jij dat het bijvoorbeeld voor nieuwe partijen waarmee samengewerkt kan worden zou helpen als er over hoe Sense met privacy omgaat gecommuniceerd zal worden met die nieuwe partijen? Of zouden ze daar geen boodschap aan hebben.

R: Deze partijen die hier staan en niet met de klanten of iets dergelijks, dus voor deze partijen zal het niet heel veel uit maken. Voor 3rd party developers misschien wel en voor ontwikkelaars van sensoren die niets met data-opslag doen en wij wel. Voor hen zal het dan zeker interessant zijn om dat als je het hebt over een besluit ben je al gauw bang dat je data lekt of dat er wat mee gebeurt. Ik denk wel dat het zin kan hebben. Hoe wij denken over privacy is één, maar security en hoeveel vertrouwen ze erin hebben is twee, natuurlijk.

I: Hoe zit het dan met de beveiliging van data?

R: Hoe zit het?

I: Is dat iets om je zorgen over te maken in de producten?

R: Nou, het probleem is natuurlijk dat je vertrouwelijke informatie verzameld en zoals je met menig systeem online ziet, je gebruikt Linux, een bepaalde virtual machine, in al die componenten kunnen exponentiele fouten zitten, dat is gewoon iets wat er altijd is. Er bestaat een mogelijkheid dat systemen data lekken. Dat je systeem gehackt wordt. Dan heb je wel veel vertrouwelijke informatie, dus ja, maar of het dan niet veilig is. Je verzamelt alle informatie die gevoelig kan zijn. Dus je verzamelt data wat je gaat gebruiken. Sense heeft veel data verzameld, terwijl heel veel data niet gebruikt wordt. Dus je moet op voorhand kiezen welke data je op gaat slaan. Je slaat telefoonnummers op van mensen die je gebeld hebt. Je kan ook zeggen ik wil alleen een getalletje met hoeveel mensen je gebeld hebt. In dat opzicht, privacy, kan het alle kanten op. Je verzamelt wat nodig is, maar wat niet nodig is kan ook verzameld worden. Dan kan het systeem een keer gehackt worden, dan staat er misschien informatie op dat voor bepaalde mensen vertrouwelijke dingen op die eigenlijk nooit gebruikt worden. Dus applicatie gezien zijn sommige dingen niet nodig, waardoor je het onnodig privacy gevoelig maakt.

## Covenant

I: Volgens mij hebben we deze vraag ongeveer gehad. Ik heb hem hier in één regel: als jij Sense zou zijn, wat zou jij dan aan de wereld willen beloven met betrekking tot privacy?

R: Ik ben Sense?

I: Ja, jij bent Sense, en jij zegt "Dag wereld, Ik ben Sense en ik beloof jullie dat als jullie mij jullie data geven, dat ik er zo mee omgaan qua privacy."

R: Je kan er vanuit gaan dat data geheel vertrouwd kan worden opgeslagen. Daar zitten bepaalde draw-backs aan, natuurlijk. We willen een bepaalde service bieden die je eigenlijk heel erg veel eisend is, vooral de aanpak van het opslaan van heel veel data die je nodig hebt. Waarbij je een heleboel data hebt, die je niet groter wilt maken door er een bepaalde incryptie op toe te passen voor snelheidsredenen. Dus, als je kijkt naar systemen die voor bepaalde applicaties toegepast worden (voor overheid etc. voor dataopslag) ik denk dat die wel veiliger zijn, omdat ze daar heel veel maatregelen voor treffen, wat qua performance heel goed werkt, maar wat voor ons niet werkt. Dus ja, ik weet niet wat ik aan de wereld zou willen zeggen is dat je data bij ons op de veiligste plek van de wereld is, maar wel wat gebruikt Sense om jouw wereld te connecten met het internet en wees niet bang dat er iets met je data gebeurt. Dat je data veilig is bij Sense. Ik

weet niet of ik dat zou kunnen zeggen.

I: Zou je dat willen kunnen zeggen?

R: Zou ik dat willen kunnen zeggen? Lastig. Ja, ik denk het. Ja, ik heb zelf niet zo heel veel met privacy van mijn eigen data als je dat ook nog wilt weten, maar ja, ik kan me voorstellen dat andere mensen dat wel hebben. Dus ja, ik zou dat wel willen kunnen zeggen. Het is niet dat ik de intentie heb om data voor onzin te gebruiken.

[41:15]

I: Als jij wat vertelt aan de wereld en dit wat jij hier getekend hebt is de wereld, welke partijen zouden daar in dat idee meegaan? Denk je dat iedereen dat zomaar zou geloven van Sense?

R: Of ze het geloven?

I: Of zou dat dan ...

R: Ja, dan hebben we het over al deze dingetjes?

I: Ja, over die dingetjes.

R: Alle losse dingetjes?

I: Alle vaste dingetjes.

R: Ja, natuurlijk, ik kan me voorstellen dat er andere mensen zijn die data willen gebruiken om statistiek over te doen voor patroonherkenning om vervolgens toepassingen te maken, maar wel met toestemming van de gebruiker. Is eigenlijk hetzelfde verhaal. Je hebt je eigenlijke data, dus ik denk dat er geen partijen zijn die anders zouden willen of denken dat wij dat anders zouden doen.

I: Wat zou er nog moeten gebeuren voordat je wat je aan de wereld belooft, dat dat ook echt zo is? Wat zou er dan nog moeten gebeuren binnen Sense of met de buitenwereld?

R: Binnen Sense... Dat is een beetje lastig, dan hebben we het over privacy of over veiligheid, databeveiliging wat erg met elkaar samenhangt. Het is niet zo dat wij wat wij ontlenen over privacy dat dat niet zo is, maar dat zegt niet dat we wat moeten veranderen aan veiligheid als het gaat om privacy gevoelige gegevens van de gebruikers.

I: Het mag gaan over privacy en security.

R: Privacy hoeft nog dat in het contract wordt aangegeven dat je met bepaalde privacy gevoelige informatie te maken hebt. Dat je daar voor tekent.

I: Een verklaring omtrent gedrag of zoiets?

R: Ja, zoiets, maar in ieder geval dat je beseft dat je in een privacy gevoelige omgeving bezig bent. En dat er consequenties tegenover kunnen staan als je daar niet goed mee omgaat. Volgens mij is dat wel zo netjes, vooral als het straks gaat groeien en er is veel werk in verzet, dat het voor een aantal mensen niet al te moeilijk is om data in te kunnen zien. En op het gebied van veiligheid zijn nog heel wat dingen uit te zoeken waarvoor we nu niet zoveel tijd hebben, zoals data-encryptie. Je hebt partijen die bedrijven testen op data-opslag infrastructuur, hoe goed de beveiliging is en dat je een keurmerk krijgt van 'je hebt het zo goed beveiligd'. Misschien dat wij ook zoiets kunnen behalen, dat we kunnen aantonen van 'kijk we willen goed met jullie data om kunnen gaan en dit hebben we ervoor gedaan.'

I: Dat je een jaarlijkse audit laat doen door zo'n bedrijf om dat te toetsen?

R: Ik denk dat zoiets wel goed kan zijn als je goed met data om wilt gaan. Als je geen goede beveiligingsmaatregelen neemt, ben je niet echt goed bezig.

I: Dan is het wachten tot het misgaat?

R: Ja, dat is misschien iets wat nog veranderd moet worden. Natuurlijk willen we dat ook graag, maar het heeft op dit moment niet onze hoogste prioriteit. Misschien ook wel 'mijne', misschien 'mijne', maar ik denk dat deze kleurtjes meer bepalen. Maar het is zeker onze visie dat we data-security belangrijk is en dat willen we ook en STAFF3 ook, maar dat het ook een beetje onmacht is om dat op te pakken en hoe we dat willen doen.

I: Is dat ook een budget-questie? Dat er misschien geen geld is om daar moeite in te steken.

[46:30]

R: Ja, dat denk ik wel. Je hebt meer mensen en mankracht nodig en dat gaat wel samen met het budget, want er zijn een aantal dingen die opgepakt moeten worden die wel geld opleveren. Maar ja, je zou kunnen zeggen dat het mijn keuze en afweging is.

I: Maar ik weet niet, ben jij in je eentje bepalend voor wat er gebeurt met de back-end?

R: Ja, in grote lijnen wel natuurlijk, aangezien STAFF3 niet heel technisch is ookal heeft hij wel een beeld wat ik moet kunnen en of bepaalde dingen goed zijn, dus ik informeer hem over dingen

die ik zou willen of dingen die nodig zijn en hij vertelt mij wat nodig is en ik zorg voor de invulling. Dus ja, ik heb wel zeggenschap over hoe het ingevuld wordt en we bepalen ook wel dat er een wachtwoord op een server zit of een key voor SSH. Dat is wordt wel door mij bepaald

I: Maar STAFF3 zegt dan "ik wil dat het veilig is"

R: Ja

I: Zegt hij dan ook hoe veilig?

R: Nee, zo algemeen is het wel een beetje. Het enige level van databeveiliging waar we het over gehad hebben en ook met Pieter Hartel van Nijmegen denk ik, die bezig is met data-encryptie, over gehad hebben wat de mogelijkheden zijn om toe te passen. We zijn er wel mee bezig geweest om dat op te kunnen pakken. Hij heeft gezegd dat het wel lastig is om het zo af te schermen dat wij daar als Sense-medewerkers daar bij zouden kunnen. Het is onmogelijk om dat zo af te schermen. Er zijn naar een hoop mogelijkheden gekeken, maar hij houdt zich wat oppervlakkig.

I: Volgensmij hebben we het wel een beetje.

R: Ja?

I: Ik hoop het. Anders kom ik terug.

## C.5. Staff 1

[936\_0299.mov]

I: Wat ik met het interview wil bereiken is eigenlijk in kaart te brengen met wie jij vanuit Sense eigenlijk allemaal te maken hebt en wat voor producten, bedrijven, alles wat er eigenlijk maar om Sense heen zit vanuit jou gezien, en ook hoe jij denkt over privacy en hoe jij en hoe Sense denkt over privacy, en hoe eigenlijk al die mensen en dingen in jouw netwerk denken over privacy. Dat doe ik eigenlijk met iedereen vanuit Sense en dan van daaruit krijg je het netwerk van Sense in kaart.

R: Dat is toch helemaal niet interessant

I: Waarom is dat niet interessant?

R: Ik niet

I: Maar jij bent ook belangrijk voor Sense. En om dat dan in kaart te brengen maken we ook gewoon fysiek een kaart met tekeningetjes. Net als dat iedereen hier in het bedrijf het leuk vindt om een kameel te tekenen, gaan we hier een netwerk tekenen. Is het tot zover duidelijk?

R: Ik denk het wel

[02:00]

I: Je denkt het wel. Okay. Als het ergens niet duidelijk is of je denkt wat een rare vraag waarom vraag je dat nou weer dan kun je dat gewoon vragen.

R: okay

## Network

I: Zou jij voor mij hier in het midden op het papier of als je het toch aan durft op het white board  
R: okay.

I: Zou je voor mij een stip of een tekening of iets van wat jij dan zelf bent neer kunnen zetten van hoi ik ben STAFF1 gewoon STAFF1 is

R: Wat zal ik dan eigenlijk op schrijven

I: Gewoon iets van wat jij bent jou netwerk beginnen te tekenen gewoon STAFF1 is goed is verder niet zo belangrijk hoe het eruit ziet. Dan is de vraag met welke medewerkers van sense heb jij het meest te maken een top drie eigenlijk.

R: gatver. Wil je dat ik dat teken?

I: of dat je dat er zo gewoon bij zet ergens ik heb ongeveer vijf zes kategorieën die ik er nog even bij wil kunnen plaatsen op hetzelfde gebiedje.

R: Met de directeur

I: Dat is goed en dat is STAFF3 okay en verder. En verder met niemand of

R: Met de medewerkers en stagiairs en dan hebben we ze ook eigenlijk allemaal gehad verder

I: Dat is goed medewerkers stagiairs. Heb je nog van die groepen in het bijzonder mensen waar je heel vaak mee te maken hebt? En dan producten, dingen van Sense waar jij in het bijzonder mee te maken hebt.

R: Wat sense maakt?

I: Wat sense maakt ja  
R: Nee het is alleen dingen  
I: Wat voor dingen test jij  
R: Ja dat weet niemand  
I: Dat weet niemand  
I: Nu indoorlocalisatie  
I: Zou je die er bij kunnen tekenen of zetten. Gewoon indoorlocalisatie  
I: Nee dat maakt ook niet uit dat eh en die indoorlocalisatie hoe kom jij erbij om dat te gaan testen.  
R: omdat DEV2 mij dat gevraagd heeft.  
I: omdat DEV2 jou dat gevraagd heeft dus je hebt dan wat dat betreft te maken met DEV2  
R: jaa  
I: Dus dan zou eigenlijk zeg maar een lijntje tussen indoorlocalisatie en DEV2 de medewerker kunnen zetten. Zou je daar een streepje kunnen zetten  
[05:00] Dan het volgende Het communiceren wat Sense is naar de buitenwereld toe heb jij daar zelf een belangrijke rol in?  
R: nee  
I: nee? Wie of wat denk jij dat er een belangrijke rol in spelen  
R: voornamelijk STAFF3  
I: voornamelijk STAFF3 oke en hoe, wat voor middelen wat voor eh  
R: auto ...[5:43].  
I: oke gniffelen/ lachen  
R: is leukste interview he van ... ..  
I: Is wel leuk hoor tot nu toe dit Dus met de auto ergens naar toe hoe zou je dat willen noemen.  
R: Hoe bedoel je  
I: Is dat direct marketing of hoe zou je dat willen noemen.  
R: Is een naam voor. account management  
I: oke  
R: relatiebeheer.  
I: relatiebeheer!  
I: Denk je dat vanuit Sense gezien dat STAFF3 de enige is die daar mee bezig is of de belangrijkste.  
R: Ik weet toch ook niet hoe belangrijk die daar mee bezig  
I: Is daar verder nog pers of media mee bezig dat je zegt nou nee wij als Sense hebben deze plekken waar onze boodschap naar buiten komt. Bijv. de website  
R: de website.  
I: Heb jij daar mee te maken met de website account  
R: Helaas wel  
I: Helaas wel  
I: Hoe  
R: Door de dingen om te gooien  
I: Dus jij zet dingen op de website Zou jij dan de website hierzo ergens neer kunnen zetten en STAFF3 ook ergens erbij  
R: Die staat er toch al.  
I: Die staat er al oke Dan mag de website ook ergens bij en dan een streepje tussen jou en STAFF3 en STAFF3 en de website  
R: Tussen mij en STAFF3  
I: oh nee, neeh Ja tussen jou en eh nee dat is al prima want STAFF3 staat eral zo vlak bij jou Dat is trouwens toch goed. Zijn er verder nog evenementen of beurzen waar jij ook als Sense zijn de mee te maken hebt.  
R: nee eigenlijk stagemarkt  
[08:20]  
I: oke die mag er ook bij. Kan allemaal belangrijk zijn kan ook allemaal niks te betekenen hebben. Gewoon om daar een beeld van te krijgen wil ik het allemaal weten. Ga je daar dan alleen heen.of zijn daar  
R: nee  
I: Ga je daar zelf heen. Wie gaat daar mee

R: DEV1, een medewerker

I: Een medewerker. oke Das goed nou ja goed. Kan fout zijn dat weet ik nog niet. En welke externe partijen heb jij vanuit Sense mee te maken?

R: Definieer externe partijen.

I: Definieer externe partijen. Dat kan Almende zijn dat kunnen ook bedrijven zijn waar producten van Sense aan verkocht of aan verkocht kunnen worden

R: Alles waar een factuur naar toe gaat en...

[09:30]

I: Alles waar een factuur naar toe gaat. Ja dat is natuurlijk heel breed.

R: Het is afwerken van facturen ...bijna alles

I: Hoe ziet dat contact eruit? Is dat bellen mailen faxen?

R: Bellen mailen post.

[10:00]

I: Bellen mailen Post. oke Wat voor soort bedrijven zijn dat vooral. waar zit Sense of waar heeft Sense het meest mee te maken. Of jij vanuit sense.

R: ...

I: Hey joh, dat is vooral om te zien van wie er vanuit Sense waar mee te maken heeft.

R: Ja dat ...poot dat is zorg.

I: zorg oke

R: zorg en welzijn

I: Dus dat is waar sense zich nu vooral bezig houdt of is dat eigenlijk altijd al.

R: Dat is waar ik de meeste facturen naar toe stuur.

I: oke ,oke Dan nu misschien de wat moeilijkere vragen. Concurrenten van Sense Zijn die er volgens jou?

R: ja.

I: welke

R: Dat weet ik niet

I: dat weet je niet

R: die heb ik niet zo op mijn netvlies

I: Die heb je niet zo dat bedrijf daar die pikken onze klanten af.

R: nee die zijn sowieso die in 2013 voorbij zien komen ...

I: Dus jij kunt nu ook niet zo een twee drie die namen

R: nee

I: Zou jij dan voor mij ergens daar sensoren / bedrijven neer kunnen zetten op dat blaadje

R: Concurrentie

I: ja concurrentie En ook nog ergens zorg.

R: waarvoor dat ...

I: Die zijn bepalend voor eigenlijk waar het beleid van Sense naartoe kunnen gaan. rustig maar. Het beleid van Sense heb jij daar zelf mee te maken?

R: nee,niet echt

I: Is het beleid van Sense ergens vastgesteld. Zijn daar documenten van?

R: Niet dat ik weet.

I: Niet dat jij weet.

R: Heb jij wellicht gehoord.

I: Nou nee misschien misschien niet over documenten. ehm ehm over documenten ja goeie vraag maar de vraag is natuurlijk naar jou toe. Wie zijn er eigenlijk beleids bepalend voor, voor waar het met sense naar toe moet.

R: Lijkt mij dat dat de directeur doet

I: Is dat dan STAFF3 of zijn daar meerdere?

R: Niet STAFF3. Lijkt mij dat de directeur STAFF2 is

I: Das STAFF2.

R: Almende

I: Zou jij STAFF2 daar ergens neer willen zetten voor mij

R: Almende

I: Almende mag ook ja. Er is dus wel beleid op een richting. of is daar zeg maar ook een over vijf jaar willen we hier zijn met Sense plan?

R: volgens mij is dat er wel qua omzetcijfers. maar  
 I: Er is dus op dit moment alleen maar een richtlijn beleid zeg maar van over vijf jaar willen we zoveel omzet hebben.  
 R: Volgens mij is er wel een vrij technisch doel  
 I: maar zijn daar ook plannen bij van dan willen we die markten  
 [15:00]  
 [Missing 5 minutes of material, however drawing of the network is intact]

## Privacy

[936\_0300.mov]

I: oke we gaan beginnen. wat eigenlijk de vraag is zeg maar gezien wat privacy voor jou is zeg maar.  
 R: Het zelf mogen bepalen wat er gebeurt met gegevens over jou.  
 I: Denk jij dat sense en producten van sense eigenlijk daar bij je passen. Denk jij dat eigenlijk iedereen die bij sense werkt daar hetzelfde over denkt.  
 R: nee  
 I: Wie denk jij dat er anders over denkt  
 R: Ik ben in het algemeen gewoon wat meer op mijn privacy gesteld  
 I: Hoe denk jij dat dan mensen bij sense daar anders over denken? Kun jij daar concreet wat voorbeelden van geven.  
 R: in dat opzicht zijn mensen toch net anders dan andere mensen. Ik ben gewoon niet zo van dat delen.  
 I: Maar andere mensen dan van sense zeg maar wel.  
 R: ja. als ik bijvoorbeeld kijk naar facebookgedrag en dat soort dingen. Dat hoeft ik allemaal niet. Vandaar ook dat producten van Sense voor mij ook niet zo snel iets zijn waar ik heel veel gebruik van zou maken. Laat ik zeggen dat ik nog al achterdochtig van aard ben.  
 I: Ja dat mag. Op zich moet dat kunnen. Denk jij ook dat zeg maar wat er voor producten bij Sense ontwikkeld worden dat die ook voor mensen zoals jij bruikbaar zouden zijn als bijv wat er door sense ontwikkeld wordt voor jou voordeel biedt en verder niet beschikbaar is voor andere mensen.  
 R: Dat is het stukje wat ik zeg, ik ben heel achterdochtig van aard  
 I: Jij denkt dus niet dat wat er door sense ontwikkeld wordt alleen maar voor jou beschikbaar is.  
 R: juist. ik denk dat er altijd een ingebouwde override zit, waardoor mensen toch wel weer bij dingen van jou kunnen komen  
 I: En jij zou dan op het moment ook al zouden dat alleen maar medewerkers precairs alleen maar medewerkers of stagiairs, het clubje wat binnen sense zit als dat alleen maar mensen zouden zijn die daarbij zouden kunnen zou dat dat voor jou acceptabel zijn. Of zou jij dan zeggen die hebben er eigenlijk ook niks mee te maken.  
 R: Voor testdoeleinden vind ik het allemaal prima  
 I: Voor testdoeleinden vind je het allemaal prima  
 R: laat ik het zo zeggen, dat ik wat gemaakt hebt, dat wil ik standaard met de rest van de wereld delen. Als ik op mijn werk ben mogen ze bijvoorbeeld best weten in welke kamer ik me bevind.  
 I: oke. Dus als jij op je werk bent is dat prima. Hoe denk jij dat de andere partijen die jij zeg maar hier op het papier hebben neer gezet bijv almende als bedrijf of mensen bij almende daar over denken  
 R: anders  
 I: anders dan hoe jij erover denkt of dan mensen die er bij sense over denken  
 R: Almende denkt er ongeveer hetzelfde over als Sense. ik denk dat er bij de hele organisatie maar weinig zijn die mijn achterdocht delen  
 [5:00]  
 I: waar komt dat vandaan  
 R: Waar dat vandaan komt? Dat is van nature  
 I: ja, dus zo ben jij  
 R: ja  
 I: Hoe denk jij dat bijv. de markten waar sense in zit: zorg, sport, het nieuwe werken, hoe dat het daar met de privacy gesteld is hoe privacy daar gewaardeerd word.

R: binnen de zorg heeft dat te maken met patient gegevens. Dus daar moet je sowieso voorzichtig mee zijn. Binnen de sport, mensen die gebruik maken van dat soort dingen hebben ontzettend behoefte aan mededelingsdrang, dus die willen ook van alles delen denk ik: kijk eens hoe goed ik ben. Binnen het nieuwe werken, werkgerelateerd zullen mensen ook wel van alles met elkaar willen delen.

I: zouden die mensen daar het heel erg vinden als die gegevens dan dus zomaar gedeeld worden eigenlijk als al die gegevens voor iedereen beschikbaar zijn. waar jij dat zeg maar wel een probleem vind.

R: In de zorg kun je dat sowieso niet maken. In de sport, ja ik weet niet hoe die mensen daar over denken, ik kan niet voor anderen spreken, maar die mensen hebben wel een hoge mededelingsdrang. Zeker als het gaat om een goede prestatie.

I: Die zouden daar minder problemen mee hebben dan bijvoorbeeld de zorg?

R: ja, [wijst naar het netwerk] Ik vind dat dit een groep is waar je die keus voor moet maken en dat deze twee groepen zelf kunnen beslissen met wie je wel en met wie je niet wilt delen.

I: Hoe bedoel je dat dat jij voor de zorg dat jij daar een keuze voor moet maken? Jij als behandelaar in de zorg? of

R: Jij als degene die omgaat met de gegevens van de patient moet zorgen dat die gegevens niet zomaar op straat terecht komen.

I: Jij moet zorgen dat het niet op straat komt, oke. Hoe denk je dat zeg maar andere bedrijven die hetzelfde doen als sense doet de concurrent eigenlijk met zulk soort wensen van bijv zorg, sport, en het nieuwe werken om zouden gaan ten op zichte van patienten denk je dat daar veel verschil tussen zit.

R: Ik heb geen idee, ik weet niet hoe het bij die bedrijven gaat.

I: dus jij denkt ook niet dat sense daar heel bijzonder in is in hoe zij als bedrijf omgaat of de mogelijkheid biedt om om te gaan met gebruikersgegevens

R: nee, ik denk niet dat Sense daar heel bijzonder in is.

## Covenant

I: Dus jij denkt ook niet dat sense daarin heel bijzonder in is. Maar stel jij zou voor sense eigenlijk bepalen hoe dat er met privacy om gegaan zou moeten worden En dat zou uitstralen naar de buitenwereld wat zou jij dan beloven, als Sense zijnde, hoe er met gegevens om gegaan wordt.

R: er moet sowieso gedacht worden aan de wet bescherming persoonsgegevens.

I: Dat is dus eigenlijk een basis waar eigenlijk alles en iedereen aan zou moeten voldoen

R: Ja, de basis. Wet bescherming persoonsgegevens dus sowieso, en dat je gegevens niet zomaar op straat komen te liggen. Dat gegevens niet zomaar doorverkocht worden aan derden. En dan bedoel ik de gegevens die herleidbaar zijn tot de gebruiker.

[10:15]

I: De gegevens die verzameld worden moeten die ook perse een doel hebben?

R: Voor wie?

I: Voor diegene over wie die gegevens verzameld worden.

R: Kijk, op het moment dat ik gegevens verzamel, dan heb ik er wel een doel mee voor ogen. Maar dat doel kan voor iedereen anders zijn.

I: maar bijv voor de indoor organisatie waar je nu eigenlijk voor aan het testen bent. Ik weet niet wat daar voor gegevens over verzameld worden.

R: In welke kamer ik me bevind en of de sensoren daarvoor een beetje nauwkeurig zijn.

I: maar daarvoor wordt misschien van je telefoon bijv je gps gebruikt of daar wordt bijv een bewegingssensor voor gebruikt of worden er geluids opnames gemaakt misschien dat het hele gesprek dat wij nu hebben daar ook voor opgenomen wordt, dat soort gegevens die worden daar dus voor verzameld. is dat dan een probleem voor jou. Of is dat zeg maar eigenlijk een heleboel gegevens terwijl misschien niet al die gegevens nodig zijn voor het doel nl. de indoor organisatie. vind je dan dat dat betreft vervelend

R: Tot ik erachter kom dat er allemaal overbodige informatie wordt, overbodig is overbodig.

I: Dan zeg jij van dat moet je helemaal niet doen.

R: nee, plus het trekt mijn batterij leeg.

I: Ja. Stel die gegevens zouden toch op een of andere manier gedeeld worden met mensen waarvan jij zegt of met partijen waarvan jij zegt maar he dat is toch niet de bedoeling hoe zou daar

dan mee om gegaan moeten worden? en stel het gebeurt wel wat zou daar dan de consequentie van zijn van zijn op het moment dat jij daar achter komt.

R: schadeclaim

I: nou ja ik weet niet, stel het zou dus wel gebeuren wat zou daar dan het effect van moeten zijn.

R: nou ja ik zou het in elk geval zeer op prijs stellen als het gemeld word

I: dus jij zou op de hoogte willen zijn eigenlijk van wie daar eigenlijk allemaal met jou gegevens omgaat, wie daar mee aan de haal is geweest.

R: het is in ieder geval voor mij belangrijk of het herleidbaar is tot mij.

I: Dat is voor jou wat jou betreft het voornaamste. Het anoniem zijn van jouw gegevens. Dat is voor jou een groot punt hoe zit dat eigenlijk voor jou met andere partijen voor zorg is dat bij lastig omdat anoniem te hebben.

R: als je voor de zorg daar iets voor verzint, dan moet je behandelaar bij je gegevens kunnen, dat is logisch. Die moet ook weten dat ik dat ben. Tot op zekere hoogte is die herleidbaarheid er wel. En dat betekent dat er dan extra voorzorgsmaatregelen getroffen moeten worden, dat mensen daar niet kunnen inbreken en met die gegevens aan de haal kunnen gaan.

[15:00]

I: En in de andere sectoren: sport, en het nieuwe werken

R: Kijk, als je het gaat bekijken vanuit de wet bescherming persoonsgegevens, dan geldt dat natuurlijk voor alles. Hoe meer persoonsgegevens je verzamelt, hoe groter jouw beveiliging moet zijn.

I: Oke, wat was ook alweer datgene wat jij wil beloven aan de wereld als jij Sense bent.

R: Ik weet het niet meer, heb ik dat gezegd? Dat er zorgvuldig met je gegevens omgegaan wordt.

I: En dat het op elk moment duidelijk moet zijn met wie die gegevens gedeeld zijn. En, maar ik weet niet of jij dat gezegd hebt, dat je op elk moment moet kunnen zeggen dat gedeelde gegevens niet meer gedeeld worden.

R: Ja.

I: Denk jij dat op dit moment dat er binnen Sense, en in de producten van Sense hetzelfde over gedacht wordt?

R: Nee, maar zij kijken meer vanuit een developerskant.

I: Hoe is dat dan anders? Vooral in producten eigenlijk.

R: Ik denk dat zij meer denken in de trend van zo snel mogelijk gegevens verzamelen, en op een stabiele manier.

I: Hoe is dat, op een stabiele manier?

R: Dat de boel niet crashed. Ik denk dat dat meer van belang is; dat ze daar meer naar kijken.

I: Dan dat ze kijken naar misschien dat deze gegevens niet heel nuttig zijn.

R: Ik kan me voorstellen dat je voor indoorlocalisatie kijkt naar het nut van gegevens die binnenkomen. Wat wij gebruiken, daar wordt ook wel naar gekeken. Nee, developers kijken er zeker anders naar. Nut zal zeker een onderdeel zijn voor ze. Maar, ja, hoe krijg ik zo stabiel mogelijk en zo snel mogelijk, zo veel mogelijk informatie naar binnen. Ik denk dat nut daar dan nog weer onder hangt.

R: Je gaat geen vragen bij zitten verzinnen?

I: Nee, ik ben geen vragen bij aan het verzinnen. Volgens mij is dit hem wel.

R: Heb je er wat aan denk je?

I: Ik ga eens even kijken. Het is vooral dat jij bij zo'n beetje al die partijen in het netwerk aangeeft dat je er vrij weinig over weet. Maar het maakt wel dat je eigen visie duidelijker naar boven komt.

[20:00]

R: Ik heb meer de visie van een eindgebruiker, dan.

I: Dat helpt om die visie meer naar boven te brengen. Waar in andere interviews meer de visie van de ontwikkelaar naar boven komt. Of bij STAFF3 en STAFF2 de visie van management of de omzet naar boven komt.

R: het formuleren van de doelen ligt meer bij deze, deze en deze [wijst op tekening]

I: Dus bij medewerkers, almende, management. Oke. Nou mooi, ik ga kijken hoe het wordt. Dit geeft in elk geval meer een plaatje van het netwerk. Was dit wat jou betreft veel te lang, of viel het mee?

R: Het viel mee, het is meer dat ik het gewoon druk heb.



## C.6. Staff 2

[936\_0304.mov]

- R: En die hebben allemaal uitgelegd wat zij nou van privacy vinden
- I: die hebben allemaal uitgelegd wat zij van privacy vinden. En als je dat dan in een netwerk uittekent kan je kijken van en ik weet van welk van die actoren eigenlijk in het netwerk wat zij ervan vinden kan ik kijken of het überhaupt binnen sense stabiel is al het denken over privacy of dat het misschien heel uiteenlopende meningen zijn maar dat dat geen probleem vormt
- R: m m
- I: of dat het uiteenlopende meningen waarbij het echt dusdanig tegenover elkaar staat dat je denk van misschien is dit niet helemaal handig.
- R: okay
- I: En dan kan het dus ook zijn tussen actoren en objecten. Je kan ook een heel netwerk tekenen waar ook beleidstukken desnoods als object erin staan, want daar is ook de mening over privacy wel of niet in aanwezig.
- R: Die beleidsstukken hebben niet zoveel met onze klanten te maken.
- I: Die zitten wat meer aan de interne kant inderdaad maar de producten bijvoorbeeld zijn weer een soort van tussen weg tussen de medewerkers van Sense en de bedrijven of andere personen buiten Sense waar Sense mee te maken heeft, omdat die software vaak samen ontwikkeld wordt. En dan is het wel interessant om te kijken of er in dat product een soort van gemiddelde tussen die twee meningen over privacy zit of dat dat er helemaal niet in voorkomt maar dat er wel over gepraat wordt dat uiteindelijk niet in het product terecht komt.
- R: okay maar dat is wat jij eraan gaat doen
- I: Dat is wat ik ermee ga doen
- R: okay

## Network

[01:30]

- I: Wat we nu eerst gaan doen of wat ik wel graag wil zien is op het whiteboard kan jij daar in het midden ergens een poppetje of een dingetje tekenen wat jij zelf bent, gewoon je eigen naam ergens neerzetten.
- R: hm nah
- I: ja dat is heel leuk
- R: een poppetje
- I: zal ik het licht even aan doen
- I: en kan jij voor mij in de links bovenhoek de drie medewerkers van sense waar jij het meest mee te maken hebt neerzetten
- R: moet je er nog een poppetje van hebben
- I: nee je mag een poppetje maken maar mag er ook een lijstje van maken hoor waar jij het meest mee te maken hebt
- R: STAFF3, DEV3 en DEV1
- I: en DEV1. En dan in de rechtsbovenhoek de producten van sense waar jij mee te maken hebt als jij zegt ik heb eigenlijk nergens mee te maken dan mag dat ook
- R: nou ja de sense app het meest en sense.nl
- I: dat is dan de website
- R: en Sense half fabricaat hoe dat noemen wil
- I: dat zijn dan dingen als iVitality, Moodie ...
- R: .Bijvoorbeeld wat we bij Ask maken, daar zit Sense in, dus dan is het niet echt de app van Sense maar iets anders
- I: okay Kan je voor mij links neerzetten de partijen die nodig zijn of die waar jij mee te maken hebt die er voor zorgen dat Sense naar buiten toe gecommuniceerd wordt. Dat mogen mensen zijn dat mogen ook objecten zijn dus de website bijv die je al rechtsboven neer hebt gezet die zou er ook prima daarbij mogen eigenlijk linksmidden
- R: Misschien moet je hier dan Sense platform noemen(rechtsboven)
- I: okay platform backend website
- R: Jannie is voor mij belangrijk en RCS die twee moet ik er ook bij zetten wat het is.

I: nou ja Jannie is communicatie medewerker Rotterdam cs vanwege de website  
R: wij zitten hier, Dit gaat over externe communicatie  
I: Ja.  
R: dat weet jij ook nou de website kan ik er ook bij zeggen okay  
I: Ben jij ook betrokken bij persberichten enzo als er iets over Sense naar buiten toe gecommuniceerd of zijn er niet zoveel persberichten  
R: ze zijn er wel, ik lees ze wel eens maar ik ben er niet direkt eh maar ik ga ze niet goed keuren ofzo  
[05:00]  
I: okay kan jij aan de rechterkant neerzetten de externe partijen waarna gecommuniceerd wordt of waarna die producten toegaan mogen ook categorieën zijn  
R: allemaal?  
I: Alleen waar jij mee te maken hebt de rest hoor ik wel uit andere interviews.  
R: iVitality beetje met Parnasia MentalShare, ask verzamelclubje zeg maar alleen ook daarbuiten wat hebben we nog meer  
I: dan waarschijnlijk ook deal en alles wat daaraan hangt  
R: jansens Sinach vind ik ook nog een betere naam.  
I: die onderste wat die heb ik nog niet eerder van gehoord  
R: een farmaceut, daar zijn we meer mee aan het lullen dan dat het een klant is  
I: het is de bedoeling dat het voor Sense dat is nog niet echt een klant. Het is de bedoeling dat het wel een klant wordt  
R: oke  
I: Wat zijn de belangrijkste concurrenten van Sense  
R: tsja  
I: als je daar zicht op hebt hoor dat eh  
R: ja maar ja ik kan wel wat noemen maar echt serieus zijn ze het niet.  
I: okay  
R: ik zie niet echt een serieuze concurrent  
I: okay En waarom niet  
R: omdat het een beetje nieuw is he  
I: ja  
R: misschien omdat we echt nieuw en heel erg geweldig produkt hebben of misschien omdat we een flirt hebben waar niemand naar vraagt  
I: ja  
R: dat weet je dan niet zo goed  
I: maar het is dus wel een gat in de markt de vraag is alleen of daar markt is  
R: Is het een gat in de markt dat weet je niet. je weet niet of het een gat in de markt is maar je weet wel dat het iets is  
I: ja  
R: dat nieuw is zeg maar en je ziet wel wat dingetjes hoor je ziet natuurlijk gewoon wat host influx ik weet niet eens meer hoe het heet tegenwoordig het is ook verkocht maar eh het is wel een beetje de standaard concurrent die we noemen zo er is ook nog iets wat sense heet ofzo geloof ik ook ik weet echt niet meer wat dat nou was hoor twee dingetjes die standaard genoemd worden dus dat dat kan je dan  
I: ja Pachube heten dan dan tegenwoordig anders zeg maar  
R: Pachube en sense nog wat zeg maar Het is nog vroeg zeg maar fans of hosting  
I: Het is maar de vraag wie er het snelste iets heeft wat eh  
R: ja maar dat is nog niet echt concurrentie nu nog he. We hebben veel meer met mobiele telefoons dan dat zij doen En eigenlijk als je Sense ziet dan met de mobiele telefoon dan hebben we al weer geen concurrentie. Dan doen zij in ieder geval al minder mee. maar goed verder  
I: Verder wie bepalen het beleid binnen Sense vanuit jou gezien. wie wat eh  
R: STAFF3  
I: en die mogen ergens in de zelfde hoek en de visie van sense wie zijn daar bepalend voor die mogen rechtsonder  
R: tja. Daar is STAFF3 weer belangrijk in, denk ik.  
I: Zie jij jezelf ook binnen die beide?

R: Ja, dat sta ik toch opzich al. Moet ik mezelf er ook bij zetten?

I: Nee, dat hoeft niet.

R: Nee?

I: Nee.

R: Als jij dat wilt, ik kan ook best wel wat aanpassen.

I: De visie is toch ooit in jouw hoofd begonnen?

R: Ja, ik ben er mee begonnen.

## Privacy

I: Dan was dat het lijstje wat ik op het bord wilde hebben. Dan kunnen we nu verder met het stukje privacy. De beginvraag: wat is privacy volgens jou? Dat is een hele open vraag.

R: De basis ervan, het uitgangspunt wat wij hanteren, is dat de informatie over iemand van iemand is. De informatie over jou is van jou. Dat is de basis. Dan hebben we natuurlijk problemen als het informatie is over een gesprek. Bijvoorbeeld deze informatie is gedeelde informatie: die is van jou en die is van mij. Maar niet van een ander. Dat kun je uit vermenigvuldigen: informatie van mensen, ja, in een interactie zegmaar, is van hen zelf. De uitbreiding als je met meer mensen betrokken bent. Dan is die van meer mensen zelf. Dat is het uitgangspunt, het begin. Nou praat je over wat meer complex. Hoe je dat kan verwezenlijken. Als je informatie wilt delen met een ander is het altijd de eigenaar die mag delen. Dan moet je hem de tools geven die handig voor hem is om te delen, maar niet meer dan dat. Dat is ook het hele principe van informatie delen: het is van iemand, dat is de eigenaar. Dat is het privacy model. En Sense laat dus makkelijk hun informatie delen met anderen, maar dan moet het ook wel persoonlijk voor hen nuttig zijn. Dan moet hij dat zelf willen. Ze moeten goede tools hebben om dat te delen, ze moeten ook tools hebben om dat ook weer op te zeggen, om te stoppen met delen. Er moet niet altijd informatie daarheen gaan.

I: Er moet niet meer informatie naar een gedeeld worden dan wat er puur nodig is voor de andere partij.

R: Dat moeten ze goed kunnen controleren. Ook in de tijd. Ze moeten goed kunnen controleren, ze moeten goed kunnen delen. Ze moeten het in feiten terug kunnen halen.

I: Hmm hmm

R: Ze moeten kunnen ontsharen als het even kan. Dat is ook een technologisch uitdagend ding. Dat komt nog niet zoveel voor.

I: Want als je iets aan iemand anders verteld en je zegt op een zeker moment 'ik wil dat ik dat niet verteld heb', dan is dat natuurlijk ook lastig om...

R: Het gaat een beetje om het vergeten. Toch zijn het wel dingen in de privacywet terugvinden: iemand heeft het recht om zijn dossier te laten vernietigen ergens. Hij heeft een keer het dossier gegeven en dan moet hij ervan op aan kunnen dat het dossier verder niet gebruikt wordt. Daar zijn technologisch gezien dingen voor. Het is wel te doen. Wat is verder belangrijk: de data die van jou is moet beschermd zijn. Die moet voldoende ge-encrypt zijn, je moet er zeker van zijn dat men er niet bij kan en die moet in zekere zin niet alleen beschermd worden tegen anderen, maar ook tegen de staat.

I: Ja.

R: Dat is een uitvoering van de privacy.

I: De data moet echt puur en alleen van die persoon zijn.

R: Zet er maar een mooi password op, die mooi gegenereerd is. En met die versleuteling kan niemand erbij. Zelfs de overheid niet.

I: En ook medewerkers van Sense niet?

R: En ook medewerkers van Sense niet. Nou, dan schort er aan de uitvoering nog van alles, maar dit is wel het idee. Dat vind ik dat we eigenlijk moeten bewerkstelligen met die privacy. En er zijn nog een aantal punten waaraan gewerkt moet worden. Het feit dat het tijdelijk moet kunnen zijn. Het feit dat het goed afgeschermd moet zijn met een password. Het moet zodanig geconfigureerd zijn dat je dat niet voor elkaar kunt krijgen. Andere dingen die ook lastig zijn: op het moment dat je aantal data deelt, dan is het relatief makkelijk om andere data te linken met data die je al hebt, dat je het steeds groter maakt. Stel dat je van een aantal Rotterdammers het woon-werkverkeer krijgt en de snelheid daarvan, maar gedepersonaliseerd. Dat is ook een belangrijk deel van privacy, de technologische uitvoering, dat heet depersonaliseren. Als ik dat precies weet, dan ben jij

natuurlijk de enige die van jouw huisadres naar Sense gaat en 's avonds weer terug. De data die daar nog aan kleeft, is gepersonaliseerd als ik eenmaal weet waar jij woont en werkt. Een ander cruciaal punt is het depersonaliseren van data.

I: Het annoniem kunnen deelen

R: Precies. Dat is een van de dingen die we nog meer willen gaan doen. Die ook voor klanten van Sense interessant kunnen zijn, omdat die gedepersonaliseerde data zoveel waard kan zijn. Bijvoorbeeld het gebruik van pillen, daar wil een farmaceut voor betalen, wanneer hij van honderdduizend man weet wanneer ze hun pillen nemen en ook weet wat hun activiteiteniveau hierachter is. Dat zou best een hoop waard kunnen zijn. Het zou een hoop mensen in staat stellen om pillen te verkopen, dus dan kun je in feite geld gaan verdienen met een Sense-applicatie. Maar daarvoor is het wel belangrijk dat ik het voldoende weet te depersonaliseren. Dus, privacy, dat is duidelijk, dan kom je dus met zorgen dat er echt niemand bij kan, dat alles tijdelijk is. En gedepersonaliseerd is een optie die we technologisch gezien zouden willen. En het delen. Dus dat het goed beveiligd is en versleuteld.

I: Maar dat je het wel makkelijk kan delen.

R: Ja, maar ook dat je het makkelijk terug kunt halen. Je moet ervoor zorgen dat mensen... Wat zei ik nou?

I: Delen van data, beveiliging, dat het annoniem moet.

R: Personaliseren. En depersonaliseren.

I: En verhandelen?

R: En verhandelen, delen. En wat is het gevolg daarvan.

I: Delen.

R: Maar goed, dat somt nog wel een beetje op.

I: En, even kijken, met betrekking tot wat er bij Sense bijvoorbeeld gebeurt, wordt er soms bij testdata heel veel data verzameld voor een toepassing waarbij uiteindelijk misschien maar 3/10 sensoren nodig zijn om die state informatie te krijgen. Zeg je dan dat het ook belangrijk is dat er niet te veel informatie verzameld moet worden? Want eigenlijk zijn dan 7/10 sensoren eigenlijk niet nodig.

R: Nee, het is juist andersom. Je weet van tevoren niet wat je allemaal nodig gaat hebben.

I: Dat is lastig om dat te selecteren?

R: Precies en dat moet je juist niet doen. Het is juist wel fijn om allemaal data te verzamelen van mensen. Langzamerhand zullen algorithmes worden ontwikkeld, waarbij data waar je aan het begin niets aan had, je toch wat mee kan doen. Uitgangspunt blijft dat het gewoon persoonlijke data is en dat het jouw keuze is wat daarmee te doen. Maar alle gedragsgerelateerde data die je nu hebt, die kan prima later van belang zijn.

I: Die kan nog toegevoegde waarde hebben voor een toepassing die je nu nog niet weet?

R: Inderdaad. Dat weet je nu nog niet. Dat zou best mogelijk kunnen zijn.

I: Ok. En voor het delen en het stoppen van dat delen is het waarschijnlijk ook handig om elk moment in te kunnen zien met wie je deelt op dat moment?

R: Nou, op zich kun je nu zien wie er op dit moment jouw data gebruikt.

I: Dus ook echt het gebruik ervan?

R: Het heeft niet alleen met delen te maken, maar hij zou het eigenlijk niet mogen opslaan. Dus hij moet gewoon iedere keer kijken. Dat is ook handig wanneer je data, bijvoorbeeld waar je woont opslaat, en iedereen kan er in kijken, dan hoef je niemand meer een verhuisbericht te sturen. Het is ook best handig, een betere manier van omgaan met gegevens.

I: Ok, hoe denk je dat de partijen op het whiteboard erover denken ten opzichte van hoe jij er over denkt? Komt dat overeen, zijn er verschillen tussen? Dan gaat het ook over bedrijven en mensen, maar ook over objecten en toepassingen van Sense zelf of daar ten opzichte van hoe jij dat graag zou zien...

[20:18]

R: Ten opzichte van het intern, als het gaat om een DEV3 enzo, die denken allemaal wel hetzelfde. Hoe Pachube en [Open]Sense erover denken dat weet ik niet, maar dat gaat ook wel die richting op. Maar die klanten, want dat zie je dan bij iVitality, Parnassia, enzovoort, die hebben allemaal hun eigen idee enzo. Dat is echt wel anders dan hoe wij erover denken.

I: Hoe is dat vaak anders?

R: Ze zien het vaak meer als een probleem. Wij hebben het eigenlijk niet zo goed doordacht nog.

Het is een wat minder volwassen kijk op de zaak. Jansen-Cilag die zou natuurlijk meer kijken wat de wet erover zegt dan de basis goed hebben. Parnassia is er wat minder bezig. In het algemeen kun je beter zeggen dat die bedrijven meer bezig zijn met wat mag nou wél en wat mag nou niet volgens de wet. Invi is ook een beetje lastig, want die heeft ook nooit in de gaten gehad dat we zoiets als mobiele telefoons en sensordata zouden ontwikkelen. Dus dat... ja eeh... dat relateren van informatie dat ... dat is lastig. Zo'n wet is moeilijk, dat is niet duidelijk genoeg.

I: Het zal vast ook niet zo zijn van stel je bent met een aantal mensen bij elkaar en je verzamelt daar data over... Is dat heel duidelijk in de wet?

R: Nee, nee, nee, nee. Je ziet dat bijvoorbeeld in de medische wereld. Dan zal zo'n arts ook vinden dat een gesprekverslag van hem is. Dat zijn zijn notities. Dan kun je het er nog hebben of je als je allebei notities maakt dat je je eigen notities mag hebben, dat lijkt me ook geen probleem. Maar stel dat hij het gesprek opneemt, dan lijkt het me verstandig dat dat eigendom van beiden is.

I: Hoe gaat dat eigenlijk op het moment dat je dat zou willen delen? Waar twee mensen rechthebbend op zijn. Moeten ze dan beiden toestemming geven?

R: Je kan beginnen bij, er vanuitgaande ze hebben allebei smartphones en de een neemt op en de ander niet, dan kun je vragen of je daar recht op hebt. Ligt er ook aan hoe je het opgenomen hebt. Misschien heb jij het wel opgenomen met 3D-camera's en heb je er veel geld in gestopt en ik heb het niet betaald want ik hoef dat niet. Dan heb ik ook het recht om dat op te nemen. Het is wel een gebeurtenis die door ons tweeën... Het gaat om principes daarin. Dat is het eigenlijk. Wat is van wie, zegmaar. Data over jou is van jou, behalve als dat uit een interactie komt, dan is die ook van de ander. Het is eigenlijk wel zo dat je probeert te voorkomen dat mensen een dossier over jou hebben hebben, waarmee jij niet..

I: Dan moet de ander op de hoogte zijn?

R: Precies. Naast dat, ja, het is natuurlijk een een-en-een-ting als het gaat om bijvoorbeeld de feitelijke gebeurtenissen en anderzijds als het gaat om de meningen. Er mogen twee mensen natuurlijk best iets over jou communiceren zonder dat ze jou daarbij betrekken. Dat is vrij normaal.

I: Dat gebeurt nu ook natuurlijk.

R: Die informatie is dan niet van jou, maar gaat wel over jou. Maar die is van die twee mensen.

I: Dat lijkt mij lastig om te moeten uitleggen aan bedrijven die daar zich niet op zo'n niveau bezig houden, maar alleen kijken naar wat mogen we volgens de wet?

R: Ja, dat is lastig. In het begin zien ze allemaal nog probleem en soms kunnen we daardoor nog geen zaken doen en anderen zien dat eigenlijk niet zo en hebben zich nog niet zo gerealiseerd dat ze er later een probleem mee zouden kunnen krijgen. Daarnaast is de wet natuurlijk continu aan het veranderen. Dat regelingen nog niet geregeld zijn. Er zijn nog allerlei dingen, vandaag stond bijvoorbeeld in de krant over privacy over vliegende robotjes, ik kan met mijn robot boven jou huis gaan hangen, het is immers mijn robotje, mag dat? Maar ja, ik mag hem ook jouw huis in vliegen, mag dat dan nog?

I: Ja, het is jouw huis.

R: Ik mocht jouw huis niet in, mag mijn robotje dan wel jouw huis in, dat lijkt me dan ook niet. Maar ja, hoe is dat geregeld? Is die robot autonoom en heeft ie het stiekem gedaan.

I: Wie z'n schuld is het dan?

R: Hoe autonoom is zo'n robot? Er zijn nog heel veel dingen die we nog helemaal niet geregeld hebben, dat weten we nog niet hoe het moet. Uitgangspunt zou informatie die direct over jou gaat.

I: Sensorwaarnemingen?

R: Ja, sensordata die is van jou. En die moet je kunnen delen of niet kunnen delen. Als iemand betaald heeft voor die sensordata dan is die data misschien ook wel voor hem, maar dan ook alleen maar die data. Niet alle informatie. Niet alle informatie is jouw informatie. Als je dat als uitgangspunt neemt kun je veel dingen wel oplossen.

I: Ok.

R: Voor ons ook, want er past wel het een en ander in die wetgeving zegmaar. Zorgen dat mensen informatie verzamelen en wij daar niks mee doen, behalve als server. Dat betekent ook dat Sense niet informatie van anderen aan een ander zou kunnen verkopen.

I: In hoeverre is daar vanuit Sense, wordt daar bezig gehouden met die wetgeving?

R: Er wordt wel naar gekeken. Maar wetgeving is een onderdeel van de ontwikkeling. We houden

ons aan andere dingen dan alleen maar die wetgeving. Natuurlijk moet je je aan die wetgeving houden, maar je moet een beetje scherper kijken dan dat.

I: Maar er is niet specifiek iemand die zich verdiept heeft in die wetgeving?

R: Nou, ik denk dat STAFF3 daar wel redelijk naar kijkt.

I: Ik weet niet jij daar heel erg in zit, maar de software en producten van Sense. In hoeverre is het daar, zegmaar het beeld wat jij hier schetst nou daar willen we naar toe werken, op welke gebieden mist er dan nog wat?

R: Nou, ik denk dat er intern wel heel duidelijke afspraken zijn wie wel wat mag en wie niet en waar je bij mag, dat kun je nog veel meer in de software verankeren. Zodat je het feitelijk onmogelijk maakt dat iemand daarbij komt. Dat geldt op al die niveau's. Dat is dat delen van informatie, het versleutelen van informatie. Hoe kan ik beveiligen zodat niemand erbij komt? Het is natuurlijk altijd zo dat iemand een algoritme maakt om te versleutelen, perfect te versleutelen. Dus hoe kom je erachter of daar een back door tussenzit?

[30:00]

I: Dat die gene die het algoritme geschreven heeft niet stiekem een lijstje heeft met exporteerbestandje heeft.

R: Precies. Dat zijn allemaal dingen die je alleen maar op kan lossen door er meerdere mensen naar te laten kijken en heel zeker weet je het nooit. Dat is het probleem met alle beveiliging, zegmaar, dat is een kwestie van ontwikkelen. We kijken niet in een keer hoe, maar er is wel aandacht voor. Daar moeten we op blijven focussen. He maar, als je naar diverse klanten kijkt of andere klanten waar ik mee praat, die zijn bijvoorbeeld heel bang dat de data, de medische data van personen die Sense gebruikt op straat komen te liggen. Dat is natuurlijk wat je echt moet zien te voorkomen, dat dat dus echt niet gaat. Dat doe je door dingen te versleutelen of toegangsbeveiliging te hebben, door daar scherp naar te laten kijken. Dat doe je ook developers research, niet alleen met afbraak...

I: Ik heb ook gehoord dat ze in de medische sector graag willen dat de persoonsgegevens op een andere server stonden dan de sensordata, omdat het dan anoniemer is. Er waren inderdaad wat strengere eisen waren uit de medische hoek...

R: Hoewel dat natuurlijk niet de beste manier is om dat te realiseren, maar ja, of dat het niet in Amerika mag staan.

I: Omdat ze daar een andere wetgeving hebben.

R: Maar als je het zou hebben versleuteld zodat niemand erbij kan, of trouwens dat is ook weer wetgeving waar je tegenop kan lopen dat dan niet mogen. Dat je data niet mag versleutelen dat niemand er bij kan. In Nederland mag dat wel, in Amerika niet. Dus dan ben je eigenlijk in overtreding, want de overheid wil die data hebben, anders ben je in overtreding.

I: Zijn er veel landen die net als Nederland zeggen als je het zo wilt versleutelen dan mag dat?

R: Voor de meeste landen is daar geen wetgeving tegen. Vooral Amerika is na 9/11 vooral losgekomen met dat verhaal, de patriot act, ik weet het niet helemaal, maar die gaat best wel ver.

I: Het is vooral Amerika waar je je data niet neer moet zetten?

R: Nouja, 'niet neer moet zetten', als het helemaal versleuteld hebt maakt het ook niet uit, maar je zou tegen het probleem kunnen lopen dat de Amerikanen dan vinden dat je heel erg opvalt.

I: Ja.

R: Duitsland is juist de andere kant op, die zijn heel erg aan de privacy kant, die letten daar veel meer op en dat wordt ook veel moeilijker. Ook privacy levert wel problemen op, zo kan je niet alles combineren. En als je dat verkeert uitlegt kun je ook niet alle projecten doen die we met Sense doen.

I: Ja. Dus eigenlijk zitten we in Nederland wel prima?

R: Dat weet ik niet. Eigenlijk denk ik dat het in de meeste landen wel kan, omdat je in de positie zit, 'de data is van jou', de vraag is alleen of de overheid jou en ons als server-provider niet kan dwingen om de data openbaar te maken en of wij niet iets kunnen doen om dat weer te kunnen verkomen, om te zeggen 'dat kunnen we niet'.

I: Als je nou een week voor een gerechtelijke uitspraak tegen al je klanten zegt 'ik zou even al je data weghalen'...

R: Dan ben je weer in overtreding, omdat je verplicht bent data een paar jaar te bewaren. Het gaat om internetcommunicatie in Nederland, alles wat je maar communiceert, iedere email, dat moet bewaard blijven.

I: Zo, ja.

R: Dus ja.

I: Dat is een hoop meer dan de papieren post, althans voor mij aan de deur, misschien dat je als bedrijf wel je papieren post moet bewaren.

R: Er is niet zoiets als briefgeheim op internet.

I: Was dat ook niet met nieuwe wetgeving, dat dat wat beter ging, dat het meer overeen kwam, de echte wereld en de internetdata.

R: Ik denk niet dat we met e-mails zover willen gaan. Wat het effect is, elke terrorist weet dat ook, elke mail wordt gescand, het gaat er wel weer omheen. Dat is natuurlijk een heel ander slag, dan communiceren ze er niet mee.

### Covenant

I: Waarschijnlijk komt het heel erg overeen met wat je net gezegd hebt over wat jouw visie over privacy is, maar als jij Sense zou zijn, wat zou jij dan aan de wereld willen beloven met betrekking tot privacy.

R: Ja, nouja, dat we het goed beveiligd hebben, dat jouw data inderdaad van jou is, dat je dat tijdelijk kunt delen met anderen, dat je het ook depersonaliseren en op die manier geld voor kan vragen, waarbij je middels depersonalisatie zo goed mogelijk gezorgd hebt dat die privacy niet geschonden wordt, in ieder geval geven we aan waar de gevaren liggen, want depersonalisatie is niet perfect te doen, want zoals ik net al zei: als ik maar weet waar je woont of werkt dan haal ik je zo uit alle vervoersbewegingen van Nederland, omdat jij de enige bent die dat doet en als daar meer data aan zit, dan heb ik een probleem. Dus dat is lastig, zegmaar gewoon zo, als ik jouw hartslag heb en ik heb nog een paar andere sensoren die delen we met elkaar en jij blijkt een beetje bijzonder patroon in je hartslag te hebben, als ik dat ergens anders weet, dan weet ik ineens nog meer over die persoon. Maar goed, dat we het zo goed mogelijk depersonaliseren, depersonaliseren beperkt in ieder geval het gevaar van privacy schending. Dat kunnen vertellen, duidelijk kunnen maken, minimaliseren. "Jouw data is voor jou", daar komt het ongeveer op neer, dat hebben we met de huidige maatstaven zo goed mogelijk verzorgd doordat het allemaal versleuteld is, dat we interne procedures hebben waarop het zeker is dat ook het personeel van Sense, techneuten, dat die daar niet bij kunnen en dat het zelfs voor de overheid onmogelijk is om dat te doen. Dat zou ik willen doen. Ik weet niet of ik dat zou redden.

I: Maar het is wel graag wat je zou willen doen.

R: Ja, het is wel graag wat ik zou willen beloven. Op een gegeven moment kan iets wat we nu zeggen tegen de wet zijn en dan kunnen we zeggen gaan we dan in dat land niets doen. Of, ja, of zeg ik dan: okee jongens, in dit land doen we het wel, maar die zien weer niet dat als de overheid komt dat we het zelfs aan hun moeten geven. Nou dan weet ik niet hoever we daar precies in kunnen gaan, maar het liefst zou ik dat zo willen beloven.

I: Eehm. Alle partijen op het white board, zouden die zich daarin kunnen vinden? Zou dat...

R: De externe partijen, MentalShare, Parnassia, daar zou ik mee moeten overleggen of ze dit voldoende vinden. Zij zullen eerder toch naar de wetgeving kijken, eigenlijk meer kijken naar wat voor risico zij als organisatie lopen in plaats van wat er nou echt op lange termijn maatschappelijk wenselijk zou zijn.

I: Dus die doen meer met regeltjes en wetten.

R: H Precies, ja. En die wetten ontwikkelen zich ook wel eens de goede kant op.

I: Denk je ook dat deze visie op privacy, wat jij nu schetst en wat jij zou willen beloven, op de een of andere manier in de wetgeving zou kunnen komen? Denk je dat Sense daar een rol in kan spelen?

R: Je ziet wel bewegingen die kant op. Want je krijgt natuurlijk je medisch dossier, zo werkt het, het wordt zo geformuleerd dat je er inzage in krijgt, in plaats van dat je er eigenaar van bent, maar het is natuurlijk wel een stap die richting op. Dat gaat precies, die stappen moeten er nog verder bovenop komen. Het is natuurlijk niet zo, laten we het zo zeggen, stel je voor dat jouw kredietwaardigheid, dat is informatie die in de loop van de tijd door jou is opgedaan, het is wel informatie over jou en van jou, je moet wel certificeren dat het de goede informatie. Je hebt er niets aan dat jij tegen een bank zegt dat je kredietwaardig bent.

I: Dan zegt de bank dat zeg je zelf.

R: Maar of jij die informatie wilt kunnen geven over jouw kredietwaardigheid, dat is wel iets wat

je zelf zou moeten kiezen of je dat zou willen geven. Als jij zeg maar iemand tegenkomt, iemand in Duitsland waar jij zaken mee wilt gaan doen en die graag dat jij hem jouw kredietwaardigheid laat zien dan is dat goed, maar dan zijn er instanties die garanderen dat jij dat niet zelf hebt lopen verzinnen, maar dat dat is ontstaan uit alle interacties die zijn geweest. Dat is niet een rol die ik vind dat Sense moet spelen, maar wel een rol die je met alle data zou willen spelen. Daar horen wel certificerende instanties bij. Wat die eigenlijk doen, is op het moment dat er iets mee te maken heeft, dan identificeren zij dat ook. Nou vind ik nog steeds dat het data over jou is en dat jij dat soort dingen zou moeten doen. En ik denk dat we moeten voorkomen dat mensen data over jou gaan verzamelen, zonder dat jij daar inzicht in hebt, maar daar is die wetgeving nog lang niet ver genoeg in. Je komt natuurlijk bij jouw BKR-registratie natuurlijk niet weten wat erin staat, maar jij moet dat kunnen zien, zonder dat iedereen dat moet kunnen zien, want dat moet jij eigenlijk weer bepalen. Maar jij hebt hem nodig op het moment dat je een lening wilt afsluiten. Dus die kant zou het op moeten gaan en de wetgeving gaat langzamerhand in die richting. Soms ook weer hele stappen de verkeerde kant op. De overheid permitteert zichzelf nogal veel meer dan eigenlijk goed is voor ons, maar je later weer spijt van krijgt.

[40:00]

I: En dan waarschijnlijk ook met hetzelfde argument als in Amerika, namelijk terrorisme.

R: Ja, die is lekker makkelijk en daarmee ga je overal doorheen en dan moet je later maar weer eens goed zien te krijgen.

I: Ja. Zijn er ook eigenlijk bijeenkomsten of iets waar Sense zichtbaar aanwezig is, die op dat gebied van de wetgeving wat meer..

R: ECP organiseert dat soort dingen en daar zouden we inderdaad kunnen praten. Maar we zijn op dat gebied wat verder met onze ideeën dan de meesten.

I: Maar dat geeft toch een mooie discussie? Of is dat niet handig om in een discussie zover vooruit te zijn?

R: Nouja, het is een gebied. Het gaat wel gebeuren, het gaat allemaal langzaam, maar ik heb zelf niet het geduld om daarbij te gaan zitten. Het komt wel. En ik denk dat wij met de huidige implementatie van Sense geen problemen hebben, juist omdat we met het principe "de data is van jou" blijven zitten en dan ook echt die data niet verkopen of verzamelen. Je zou geen model a la google kunnen hebben. Google meet gedrag op het internet..

I: Om alleen maar vaste informatie..

R: Maar wij gaan verder met ook echt al het gedrag. Wij gaan veel verder en als je dat niet met echte privacy weet te beschermen dan heb je daar echt een probleem. Dan krijg je een vertrouwensprobleem.

I: En dat is niet wat je wil hebben?

R: Dat zou commercieel gezien heel onverstandig zou zijn. Want een heleboel mensen die als je ze Sense laat zien, schrikken wel over hoeveel ik nu weet.

I: Ja.

R: Maar als je vertelt hoeveel je van jezelf weet, dan is het minder erg.

I: Ja, als ik wil weten waar was ik vorige week ook alweer, dan zou het fijn zijn als ik dat meteen terug zou kunnen zien.

R: Ja en als jij bepaalde dingen van jezelf zou willen delen met anderen dan is dat ook prettig. Als je wel of niet op kantoor bent, bijvoorbeeld in plaats van waar je de hele dag bent. Dat is een van de belangrijke functies van Sense, dat je dat filtert. Dat je alleen maar je statusinformatie communiceert, i.p.v. locatie communiceert.

I: Dat je eigenlijk een afgeleide publiceert?

R: Ja, dat je heel makkelijk kunt kiezen wat je wel en wat je niet wilt delen met anderen en in allerlei verschillende groepen. Maar dat doen we nu natuurlijk toch allemaal. Als we nu in de buurt zijn, zien we het toch allemaal. We delen eigenlijk al heel veel informatie met elkaar, wanneer je elkaar toevallig ziet.

I: Wanneer ik op kantoor ben, zie ik wie er allemaal is.

R: Dat zijn allemaal al dingen, maar je hebt ook allemaal internetdingen, je zit op facebook, dan heb je ook allerlei informatie impliciet. Daar gebeurt van alles. Op het moment dat jij iemand belt, deel je ook informatie en als ik achter de telefoon zit en ik roep wat, dan hoort hij ook en er is natuurlijk, impliciet wordt er van alles en nog wat gedeeld, maar je moet goed nadenken wat het betekent wanneer je heel veel meer data van iemand hebt.



I: Ja.

R: Ja, je kan in de fysieke wereld ook even uitstappen: ik ga een dag niet op straat. Ik vind het allemaal eng en dan deel je wat informatie. Maar, weet ik veel, ik heb een enorm pokdalig gezicht en ik wil niet dat alle andere mensen die informatie krijgen dus ga alleen in het donker naar buiten. De dingen die daarop lijken in de digitale wereld daar moet je ook dit soort mogelijkheden voor geven.

I: Dat je in het donker naar buiten kan?

R: Ja precies.

I: Dat je niet alles deelt...

R: Ja, precies en daar kan Sense een goede rol in spelen.

[45:00]

I: Ja, maar ik denk ook wel dat die metafoor met de echte wereld een fijne is om daarin te gebruiken. Want dan hebben mensen er een veel beter beeld van van wat ben ik nu eigenlijk aan het doen.

R: De echte wereld is ook niet perfect. In de echte wereld is er nog wel paternalisme aan de gang. Over data in de medische wereld vindt men nog steeds dat de dossiers van de arts zijn, terwijl jouw adresgegevens zijn ook van jou, niet van de overheid. Het is niet dat de overheid... Het GBA, stelt ook min of meer een bestand op dat zij bepalen waar je woont. Ook als je ergens anders woont dan waar je ingeschreven staat, bepalen zij waar je woont en dat is gelul natuurlijk, je woont er niet. Wat bedoelen ze nou? Dat is de oude inschrijving of een valse inschrijving.

I: Je mag toch zelf zeggen waar je woont?

R: Eigenlijk mag je dat gewoon zelf weten. Je mag het zelf zeggen. Nou, natuurlijk moet zo'n overheid dat natuurlijk weten. Die moet dat kunnen controleren of het verschil maakt dat je thuis woont of een eigen huis hebt, dat scheelt weer bij de studiefinanciering en dat soort dingen. Maar je wilt wel gewoon de echte dingen. Laat dat bij die persoon liggen, dan wordt het allemaal een stuk makkelijker.

I: Dan het communiceren bij de overheid?

R: Ja, precies. Dan kun je certificeren waar je woont, dan laat je een instantie dat doen. Die gaat dan naar jouw huis toe, die overhoort jou over je spullen, kijken in je pasjes en zeggen: ja, hij woont hier echt. Als je dat zou willen dan heb je dus niet alleen verteld waar je woont, maar ook gecertificeerd. En dat is eigenlijk wat ze doen, de overheid, maar ze begrijpen het niet helemaal. Zeker, omdat het in de loop van de tijd zo ontstaan is. Maar dat is een beetje, ja, een beetje andersom eigenlijk. Jouw informatie is van jou. Het is voor jou relevant om te vertellen waar je woont, want jij krijgt daar post en als de overheid wil weten waar jij woont en ze willen dat zeker weten, dan moeten ze een moment kiezen waarop ze dat zeker weten en dat is het moment van jouw aangifte daar en is een certificering van, en niet meer dan dat

I: Desnoods komen ze aanbellen, dat is ook prima.

R: Precies. Ze kunnen je natuurlijk verplichten dat als jij bij ons in het land komt wonen dat je dat dan moet komen vertellen en ze kunnen je ook verplichten dat je dat binnen drie dagen moet doen en als je dat pas na drie weken doet dan ben je in overtreding, maar ja, dat blijft in feiten dat je al drie weken ergens anders woont en dat moet je onder ogen zien.

I: De vraag is dus wat hebben zij er voor belang bij om te weten waar je woont. Dat is dus voor die uitkeringen.

R: Ja, er zijn een aantal regels die daarmee te maken hebben, je huursubsidie en andere dingen die daaraan hangen. Dat moeten ze dus dan weten. Goed...

I: Kortom, jij zegt Sense is op de goede weg naar wat jij wil beloven met betrekking tot beveiliging van de data, dat de data van jou is, dat je het moet kunnen delen voor de periode dat je het zelf wil, het depersonaliseren en het daaruit voort vloeiend verhandelen van je data. Jij zegt, dat komt goed, wij zijn niet hele vreemde dingen, het is hoogstens dat als de wetgeving ineens zegt dat wat wij willen niet kan, dan zou dat een blok zijn, maar verder zie jij geen onmogelijkheden.

R: Ja, het is wel...

I: Denk jij dat er genoeg moeite in gestoken wordt bij Sense?

R: Er is te weinig tijd, we hebben te veel te doen. Dat zou best wat meer kunnen. Ik denk dat er wel een cultuur heerst, waarbij nouja dat van reguliere procedures dat klopt wel, maar dat zou toch wat meer in de software terecht kunnen komen en er moet echt wat meer aan de versleuteling gedaan worden. En dat gaat een beetje langzaam en dat heeft ook te maken dat

er andere dingen belangrijker zijn, maar nou is het ook allemaal niet zo heel slecht vergeleken met andere systemen, dan doen we het best wel waardig, maar als we echt zo'n privacy systeem zijn vind ik dat we daar wel wat meer aan zouden willen doen. Ik vind ook wel dat er nog wel een onderwerp is, zoals het tijdelijk beschikbaar stelen van data en vrij gegarandeerd zijn dat je het weer terugkrijgt. Kijk, je kan dat met wetgeving afdwingen, dat je data maar een keer mag gebruiken, maar dat is nu niet te doen. Dat kun je alleen maar contractueel afdwingen. Je moet er keer op keer een handtekening onder zetten en dat zou je ook weer moeten controleren. En dat is heel lastig. Je zou het wettelijk kunnen afdwingen, maar ook een deel technologisch kunnen afdwingen, dat laatste vind ik interessant om een verdere research op te leggen. Dat je data precies een keer geeft en dat je het alleen die keer kan gebruiken en het onthouden ervan geen zin heeft.

I: Dat het bewaren ervan zinloos is. Een soort James Bond videobandje, waarop staat 'je mag dit een keer luisteren en dan viegt het in de fik.'

R: Ja.

I: Dat is wel interessant.

R: Omdat elektronisch te doen.

I: Ok.

R: En dan nog een ander ding is gewoon om te zien hoe vaak dat is gebruikt, een analyse, dan kun je laten zien hoe vaak die gebruikt wordt. Bijvoorbeeld een medisch dossier en iedereen die er in kijkt en je laat hem open, dat je kan zien hoe vaak hij wordt gebruikt. Dat is prima wettelijk af te regelen. Het is helemaal niet erg dat je kijkt, maar je moet wel even laten zien dat je kijkt. Als je gewoon alles logt; als de dokter in jouw file zit te kijken, dan wil je dat weten. En als hij niet in die niet in jouw file kan kijken zonder het jou te laten weten, dan denk ik dat het een aardige privacybescherming wordt.

I: Ja, want dan kun je ook zien of er misschien andere dokters die helemaal niks met mij te maken hebben in mijn dossier aan het kijken zijn.

R: Ja, dit wordt nog een heel gebied, waarbij nog een heleboel technologische ontwikkelingen volgen. Dit wordt nog een heel gebied, waarbij nog een heleboel technologische ontwikkelingen volgen en dat is natuurlijk bij privacy of in ieder geval bij versleutelingen, dat is een gebied waarbij je continu verder gaat. Ieder systeem dat je bouwt kan gehackt worden.

I: Dat zorgt ervoor dat je weer andere aanpassingen moet doen.

R: Ja, dat is het werk. Continu veranderen. Als we echt verder komen in dingen als quantum computing, dan moeten we weer hele andere beveiliging gaan doen.

I: Dat wordt dan weer een uitdaging. Okay, dat waren ongeveer mijn vragen. Heb jij nog dingen waarvan je zegt: dat mis je nu nog, dat moet je echt nog weten.

R: Ik denk dat je een redelijk compleet beeld hebt.

I: Ja. Je hebt een hoop verteld, dat helpt.

R: Klopt het allemaal nog een beetje?

I: Ik denk dat het allemaal nog wel een beetje klopt.

R: Krijg je van iedereen hetzelfde verhaal?

I: Ja. Iedereen is goed opgevoed. Het stukje depersonaliseren kwam bij jou veel meer naar voren dan bij anderen.

R: STAFF3 ook niet zo?

I: Wel verhandelen, maar depersonaliseren dat dat daar voor nodig is of dat dat daarvoor handig is werd niet expliciet genoemd.

R: Nee, maar dat is, dat is ook een leuk technologisch vraagstuk. Het is niet een waarvan ik denk dat is helemaal klaar.

I: Er zijn al papers over geschreven, maar het is nog niet af.

R: Het is zeker nog niet af, het is ook nog niet overzichtelijk, maar het is zeker een interessant probleem.

I: Dat maakt ook weer, dat is het ook weer het leuke dat Sense aan Almende hangt, dat je ook continu met onderzoek bezig kan zijn om dit dan weer verder vooruit te helpen.

R: Ok, maar je hebt nog geen klanten gesproken?

I: Nee, ik heb nog geen klanten gesproken. Ik denk dus dat ik op basis van de interviews die ik gehouden heb, ga ik kijken welke klanten er bepalend zijn of waar wordt het meest mee samen ontwikkelt en dan denk ik dat ik daar een stuk of drie van wil spreken.

R: Het levert ook erg andere beelden op. Ik zeg nou wel heel erg dat iemand heel erg over wetgeving zeuren of die heeft er niet goed over nagedacht. Ik denk ook dat dat zo is, maar ja, hoe zeker... Bij sommige klanten is het wel goed. Maar ik denk dat de meesten vooral naar de regels zitten te kijken van wat mag er nou wel en wat mag er nou niet.

I: In plaats van waar wordt mijn klant blij van?

R: Ja, precies. In plaats van wat zou nou goed zijn in de wereld. Wat is nou verstandig. Ik ben, en een van de dingen waar ik echt bang voor ben, met name met dit soort data is dat de staat...

I: Dat die dat uiteindelijk wil hebben. Dit soort data wil hebben voor weet ik veel wat...

R: Weet ik veel wat voor politieke consternatie we over twintig jaar hebben, dat kan alle kanten op gaan. Die hebben in principe de mogelijkheid om heel veel, ze brengen het ook allemaal naar de bron. Het is net als dat je een centraal geleide economie een vooroorlogse economie, dat houdt allemaal kort stand, maar je kan wel tien, soms wel vijftig jaar enorme ellende hebben. Het is niet de meest productieve manier en het blijkt dat we er iedere keer wel weer uit groeien.

I: Het zou mooi zijn om dat te voorkomen.

R: Keer op keer als er een nieuwe technologie komt, dan is er de mogelijkheid om het verkeerd te gebruiken. Nou is dit wel een technologie die dictators in de weg zit, want het maakt het heel erg mogelijk om te monitoren waar mensen mee samen werken. Het is allemaal controleerbaar. Het is wel mooier, maar als je die sensordata overhoudt en je slaat die communicatie plat, die verbied je of weet je tegen te houden, ja dan kan het ook weer verkeerd aflopen.

[57:35]

[93010304.mov]

R: dus ik ben eh daar nog al eh

I: jij wil vooral de data beschermen tegen de overheid

R: ja vooral dat ja en dan vooral de grote overheid verkleinend tot gemeenten je bedrijf noem maar op ik vind het niet erg dat je sommige data als je aan kan tonen waar je het voor nodig hebt ik vind het prima dat een bedrijf een koeriers trackt en traced. dat lijkt me helemaal goed maar dat gaat dan wel als volgt. je wordt daar koerier en dat je dan zegt hier heb je een mobiele telefoon dat is dan jouw data bij ons bij sense ja en dan moet de koerier bij Sense zeggen de gps informatie wil ik wel delen met mijn bedrijf. dat moet ie zelf doen dan is dat eigenlijk geen probleem. Als je aan de andere kant zegt dat wil ik niet dan is dat ook geen probleem dat je baas zegt dat is dan leuk dan heb ik ook geen werk voor je.

I: Dat is zeg maar een voorwaarde om daar te gaan werken

R: ja dat is een voorwaarde om daar te gaan werken maar dat vind ik ook een reelee voorwaarde.

I: ja

R: op het moment dat ie zou zeggen nou ja ik wil je hartslag de hele tijd hebben. dat vinden wij maatschappelijk niet zo'n goed idee dat je baas je hartslag de hele tijd ziet

I: En verzekeraars vinden dat al helemaal geen goed idee als ie dat wist

R: precies dat kunnen je gewoon regelen. ja verzekeraars daar kunnen we over praten vinden we dat goed dat ze dat allemaal te weten krijgen. ik denk dat we dat niet goed vinden. Daarom hebben we ook algemene verzekeringen. Het hele punt van verzekeren gaat natuurlijk ook wel een beetje weg als ze alle data hebben.

I: Dan zeggen ze oh jij hebt zo'n risico hier op en zo'n risico daarop nou wordt jouw premie ?.....dan geef ik jou een tientje

R: dan had je ook geen verzekering meer hoeven nemen want dan betaal je wat je het echt toch gaat kosten Dat is een beetje het gene waar ik het meest bang voor ben nou ja bang. dat is waar je aandacht aan moet besteden

I: dat is de nou waar zij niet bij zouden moeten

R: dat het individu beschermd wordt dat het is heel fijn dat je allemaal informatie over jezelf verzamelt maar het is wel van jou. Ik denk ook anders om hoor commercieel gezien op het moment dat je het anders om zou inzetten dat er ook heel veel individuen zouden zeggen ja dan doe ik het niet. logisch toch

I: ja het leuke hier aan is dan wel weer dat je dus als individu wel kan zeggen van ja nou he voor mij is die dart eigenlijk niet zo heel erg belangrijk als andere mensen dat weten die mogen dat best van mij kopen of inzien. als je dat maar wel bewust hebt

R: ja

I: ja das wel mooi ja

R: dat kan inderdaad ook waar zijn daardoor ga je meer met elkaar samenwerken. Dan ga je meer Stel dat jij altijd leuke natuurwandelingen maakt ofzo. nou mooi prima die wil je wel delen met anderen dat gaat dus eigenlijk van zelf op die manier. wil je misschien ook nog de foto's die je gemaakt hebt delen ofzo en dat is dan ipv de vroegere anwb wandelroutes. weet je wel zo en iedereen heeft zo zijn eigen nou dat soort dingen

I: Dan krijg je op een gegeven moment van he de meeste mensen lopen deze route die zal wel het leukste zijn Dat is met die activity tracker waar DEV2 nou mee bezig is

R: Ja dat is ook zoiets

[03:30]

I: je loopt de deur uit en automatisch wordt het een wandelroute

R: ja ja precies een heleboel dingen gaan vanzelf. maar dat geldt straks ook voor dingen als pil gebruik je humeur wat er aan vast zit of bepaalde activiteiten nivo dat kan voor mensen in de onderzoekssfeer nogal kan dat wat waarde hebben. En dat ze hier eens kunnen zeggen met van joh wat voor pillen gebruik je en nogal wat marge dan men er wat af doen dan krijg je 20 procent korting daar kun je voor kiezen moet dat wat waard zijn. Dan moet je wat wreder zijn bijv dat dat voldoende gedeneutraliseert ????? is ofzo

I: ja

R: en dat je niet allerlei last krijgt van data die je aan de pfarmaceut hebt verkocht en je die dan vervolgens dat via de verzekeraar ineens eh dan heb je 20 procent op je pillen bespaart en gaat je verzekering met een graad of twee omhoog dat schiet dan alweer niet op. Je moet daar goed over nadenken de uitgangspunten vooral de eerste deze data is voor jou en voor jou .en als je dat uitbreid naar een groep mensen, dan is die van die groep mensen. Dan denk ik dan kom je er wel uit.

I: Wil je trouwens ook nog dat die data dat mensen die zelf kunnen veranderen als ze dat willen

R: ja dat is een van die dingen die ik ook belangrijk vind. Dat is een eh ook een bescherming. Sommige data moet je. Alle data moet je kunnen veranderen behalve als je een gecertificeerde instantie hebt . je moet natuurlijk die waardigheid niet kunnen veranderen. je mag er ook één maken die jezelf verzonnen hebt Je moet dat dus die data .Als je niet de stempel van een ander wilt hebben moet je het kunnen veranderen.Het grappige daarvan is dat je dus in feite gewoon een ultimate alibi generator kunt maken zo dat maakt je privacy ook wat beter Maar die data is van jou.,waarom zou je .....

[05:40]

I: Als ik aan jou wil vertellen dat ik vandaag lekker thuis heb gezeten. ja dan mag dat

R: dan mag dat en als ik denk ik vertrouw het niet dan mag ik er een certificerende instantie bij roepen

I: of je moet bij mij thuis aanbellen

R: dat kan ook. precies dan moet ik dat onderdeel controleren dat mag ik dus gewoon altijd doen omdat het jouw data is. ik zal het je nou jouw data verkoop zeg maar gewoon aan de pillenboer ik geloof het wel daar moet ik op vertrouwen je je gaat toch niet alles lopen veranderen en dat zou kunnen dat wel maar dan wil ik wel gecertificeerd hebben dat daar niks aan veranderd is ofzo dat zou kunnen dan zou je ergens over na moeten denken hoe je dat zou moeten doen er zou tpo iemand moeten controleren dat dat niet veranderd is

I: dan zou je ergens een certificatie module binnen Sense

R: ik zou het binnen Sense kunnen doen maar ik denk, ik zoek het meer buiten Sense Binnen Sense heb je .....

[06:45]

I: ja

R: maar ja goed dat hebben we nu ook grappig aan de hand van foto's he foto is een enorm bewijsmateriaal. altijd geweest weet je wel foto effen dat is het helemaal gewoon duidelijk zo Maar ondertussen is die fotoshop activiteit zo sterk en groot geworden dat eigenlijk foto's gewoon geen enkel bewijs meer hebben je wil aan kader boxen zijn ?????maar je kan niet meer zien aan die foto dat het gebeurd is.

[06:59]

I: Dat jij kan zeggen he maar jullie denken dat ik ergens een misdrijf in Rotterdam aan het begaan was nee ik was in new york kijk maar een foto van mij in New York op die datum

R: dat telt dus niet meer dan

I: nee

R: Dat is ook wel weer mooi. weet je wel daardoor wordt het ook weer minder de tijd ook weer minder belangrijk dan. minder privad.

I: ja

R: maar het sluit aan bij de data is van jou dan mag je het dus ook veranderen je mag het deleten je mag er vanalles mee doen wat je wil je mag hem mooier maken. Het is jouw data.

I: ja ik vind het helemaal mooi

R: goed das wel weer genoeg. ja dat is wel leuk omdat helemaal op te schrijven. Ik ben wel benieuwd wat je met die klant vind?????

I: Ik zal kijken wat daar uit komt. Dus eh das allemaal mooi.

## C.7. Staff 3

[936\_0303.mov]

R: Gaan we het opnemen?

I: Ja we gaan het opnemen. maar alleen ik ga er naar kijken. Zelfs STAFF1 vond het goed dat ik het op nam. Ze zei dat als ik het ergens terug vind dan hak ik je hoofd eraf. of zoiets

R: Dat zou zo maar kunnen dat ze dat gezegd heeft. Goed. Genoeg pennen?

I: Ja genoeg pennen. Jij mag op het whiteboard tekenen.

R: okay

I: Ja want wat ik ga doen is eerst een vraag stellen over eigenlijk hoe van uit jou gezien zeg maar Sense en het netwerk waar Sense zich in bevindt en hoe het netwerk eruit ziet. Vervolgens gaan we het hebben over privacy en wat dat dan voor jou is en hoe je dat dan ziet in relatie met sense en vervolgens of dat past bij de elementen die in dat netwerk zitten.

R: Okay

I: of daar misschien inconsistenties zitten.

R: okay

## Network

I: Dus. Nou Dan wil ik je vragen om bij het whiteboard te gaan staan en dan mag je in het midden een poppetje of een dingetje tekenen wat jezelf voorstelt. okay. Dan mag je links boven de drie medewerkers van Sense neerzetten waar jij het meeste contact mee hebt. Of waar jij het meest mee samenwerkt.

R: tjsoe drie dat vind ik nogal arbitrair

I: ja

R: verschrikkelijk arbitrair.

I: Ja. Ik vraag iedereen drie. Als ik ga zeggen de medewerkers met wie ik contact mee heb dan krijg ik het hele lijstje en dat eh...

R: nou ja laat ik maar eventjes drie even doen zo. Die ontwikkelaars die zitten eigenlijk allemaal wel een beetje in dezelfde lijn denk ik. Ik denk eh ja die andere is allemaal wel een beetje in hetzelfde dat wisselt per project he.

I: Mag ook zo hoor. Dat is ook prima.

R: ik eh

I: Als je zegt de rest dan eh

R: Ja Het maakt allemaal eigenlijk niet uit Ik neem er gewoon drie.

I: Oke. Voor jou is het eigenlijk dat iedereen

R: Ik denk dat het elkaar niet veel ontloopt en dat ik iedereen even vaak spreek.

I: Okay. Dan rechtsboven welke producten en diensten van Sense heb jij het meest mee te maken of heb jij mee te maken. uberhaupt.

R: STAFF3 Ja alles.

I: wat is er allemaal dan?

R: Mag ik kiezen ergens uit?

I: Nee nee nee je mag niet kiezen Het is een open interview je mag zelf kiezen eigenlijk

R: Het is maar net hoe je het in deelt We hebben common sense (subscriptions). En we hebben nu sense apps he.

I: Is sense app dan de app die zeg maar Sense zelf gemaakt heeft of ook de apps die in samen-

werking ontwikkeld zijn?

R: (veegt uit) Ja misschien is dat beter inderdaad. Ehm discriptions, developers, publications, dit zijn weer users, en dan heb je projects, en dan heb je healthcare Wat ik hier mee bedoel is hier doen we projektmatig betaald voor de efforts om iets te bouwen hier worden we betaald om de situatie te hosten van gebruikers en hier helpen we mensen om eh eh

I: dingen te doen?

R: om dingen te doen. Op basis van Sense het zij sensor data's ontsluiters tot topsensoren of sensoren in voetbalvelden of applicatie gebruikers zoals inderdaad een time out of een hoodie zoals nu. Het zijn meer een soort van business modellen ofzo

[05:00]

I: Het is wel waar Sense zich mee bezig houdt. Links midden wil ik graag alles en iedereen die betrokken is bij het extern communiceren van Sense. Of waar jij bij betrokken bent voor het extern communiceren voor Sense. Ik neem aan dat jij zelf wel dingen doet.

R: Ja

I: Zijn daar ook evenementen of ja zeg maar momenten wanneer dat echt gebeurd

R: Ja die zijn er.

I: Zoals

R: Moeten die hier ook bijstaan?

I: Ja die mogen er ook bij staan. die mogen wel in een ander kolommetje hoor

R: Praatjes, conferenties, beurzen, magazines, weblogs. Dat is het wel zo'n beetje denk ik

I: okay. En de website van Sense

R: de website natuurlijk jaja oh je wilt dat ook nog ja

I: Zeg maar De middelen die je gebruikt.

R: filmpjes, website.

I: Dan aan de rechterkant wil ik wel graag de externe partijen waar jij vanuit Sense mee te maken hebt?

R: Bij naam?

I: Nou je mag ook categoriën noemen. Dat mogen zeg maar partner bedrijven zijn dat mogen klanten zijn eindgebruikers als je daar mee in aanraking komt.

R: (schrijft op) ja

[08:00]

I: ja? Dan wil ik zo wel links onder de belangrijkste.of eigenlijk de concurrenten van Sense.

R: (schrijft)

[09:00]

I: okay en wie zijn er bepalend voor het beleid van Sense.

R: hart?

I: Mag midden onder

R: Wie zijn er bepalend?

I: Ja Wie of wat. Dat mag allemaal

R: Bepalend

I: Bepalend

R: Je bedoeld via middelen of wie bepalen het beleid van Sense

[10:00]

I: Allebei als je dat onderscheid daarbij kan maken. Tenminste ik neem aan dat er uiteindelijk mensen het beleid bepalen maar dat er misschien ook andere dingen bepalend zijn. Zijn daar markten in het bijzonder?

R: Nee dat valt onder het kopje met opportunities

I: Ja, dus waar kans ligt dat eh

R: Maar dat gaat gewoon fundamenteel naar opportunistisch zeg maar dat is een schaal. Sommige dingen zijn natuurlijk redelijk opportunisties van ja we doen dat eerst om dat dat eenmaal nu gevraagd wordt. Andere dingen zijn gewoon heel principieel van data kwestie van gebruiker en niet zelf. en dat heeft niks met die opportunistisch in de markt te maken. Maar vooral met hoe je vind hoe je dat dat soort beperkingen moet zien. En ook bijvoorbeeld .... dat is ook rol bepalend

I: Dus dat zou dan eigenlijk dit clubje (links onder)mensen kunnen zijn

R: En beschikbare tools. Zonder smarphone zou het bedrijf niet veel kunnen

I: de soft- en hardware die er beschikbaar is en wat daar de mogelijkheden van zijn

R: De technology environment. zou ik misschien beter kunnen schrijven technology environment. heel veel componenten van dingen die in andere omgevingen ontwikkeld worden. Daar ben je toch ook een beetje afhankelijk van op welke manier.

[12:10]

R: Moeilijke vragen trouwens

I: ja zijn het moeilijke vragen?

R: Ja leuk.

I: Wie bepalen dan uiteindelijk het beleid? En in wat voor vorm komt dat dan terecht. Is daar een document van en wordt er gewoon geleefd of hoe zit dat.

I: vooral het laatste maar of dat voldoende is weet ik niet

I: Ik weet het ook niet. Okay. En nou nog een vraag die misschien een beetje overlapt de visie van het bedrijf dat is net even weer anders dan het beleid. is dat het zelfde clubje of is dat groter is dat kleiner Wie bepalen de visie?

R: Bij de visie valt denk ik dit af.(bord) Wordt kleiner. beschikbare tools is ook kleiner tot niets zou ik zeggen development roadmap die eigenlijk dan ook niet en die komt eigenlijk een beetje terug via STAFF2.

I: Is dat een document?

R: Nee Nou ja dat komt terug in de vorm van [illustreert met handen een sturende richting]

I: Nou ja dat STAFF2 weet wat er waar gaande is

R: Bijv. Stefen zit er iedere week in bij ask en Achmy die werkt er vrijdags aan met die de grote lijnen worden daar afgesproken en ook de korte lijntjes worden door de mensen direct gedaan.

I: Je bedoelt met een development roadmap daar mee dat Sense weet wat er bij de dochteronderneming op de planning staat.

R: een aantal uren willen ze half juli of eind juli een eerste versie van page pentrol page hebben bij ask en die moet ook de toestand snappen en eind augustus moet die echt professioneel beschikbaar hebben voor consumenten en dat betekent dat als ze dat besloten hebben dat ze dat gaan doen daar zit dus ook een stukje functionaliteit in van Sense dat dan bepalen hoe ze werken. Dat betekent dat wij ook bepaalde dan kun je zeggen dat doen we niet, maar over het algemeen zeggen dan van dat doen we wel. Omdat ondersteunen we ook omdat die dochter, die zuster eigenlijk de belangrijkste partners zijn daar doen we zoveel mogelijk business mee die wil je zoveel mogelijk helpen. Dus dat betekent dat als zij het in hun hoofd hebben gehaald om dat prioriteit te geven, wij ook zullen moeten kijken hoe we dat voor elkaar krijgen. Of als TNT Fix af moet omdat Rotterdam CS uitbreidt, dan moet DEV3 dus ook aan TNT Fix werken om te zorgen dat dat af komt bijvoorbeeld.

I: Eigenlijk het stukje gemeenschappelijke deadlines hebben?

R: Maar ook het type states wat je wilt herkennen komt voort uit de vraag die Ask heeft. Bereikbaarheid en beschikbaarheid is voor de zorg wat minder belangrijk, maar voor Ask wel. Dus het bepaalt niet alleen de gemeenschappelijke deadlines, maar ook wat voor soort implementaties of wat voor soort interfaces of gezamenlijke authenticatie of weet ik veel... Ja.

## privacy

I: Qua wat er allemaal in het netwerk zit hebben we nu alles van mijn vragenlijstje gehad. Dan gaan we nu weer zonder het whiteboard verder. Ik wil nu vooral weten, we gaan nu de vragen over privacy doen. Wat is volgens jou privacy?

R: Wat is volgensmij privacy?

I: Inderdaad. In jouw wereld.

R: De definitie van?

I: Ja.

R: Zo.

I: Er is geen goed of fout, het is om te kijken...

R: Tuurlijk is er een goed of fout.

I: Vast wel, maar dat hangt af aan wie je het vraagt. Je mag ook losse termen noemen.

R: Ik denk dat privacy te maken heeft met het feit dat je een bepaalde autonomie hebt als persoon en daarmee controle over informatie en data die van jou beschikbaar zijn al dan niet beschikbaar zijn voor anderen. Het is net zoiets als integriteit van het lichaam, waarbij je de baas over je eigen lichaam bent tot op zekere hoogte. Totdat je als oudere in een verzorgingstehuis verschijnt.

Die grenzen verschuiven aan de hand van de context, maar in principe is het uitgangspunt dat je lichaam van jou is en dat jij bepaalt wat er mee gebeurt en datzelfde geldt voor privacy in hoeverre mensen informatie en data kennen en hoe ze jou kunnen beïnvloeden.

I: Dat is redelijk.

R: Redelijk?

I: Als het dan over privacy gaat met betrekking tot wat Sense doet en wat Sense is? Dan gaat het over data verzamelen en opslag. Zijn er dan nog specifiekere wensen of eisen aan om te zorgen dat de privacy van de gebruiker gewaarborgd blijft?

R: Ja, daar zijn specifieke wensen en eisen aan. Daar werken we hard aan. Bijvoorbeeld de autonomie en controle betekent ook dat je inzicht hebt in welke data van jou is en met welke je die kan delen en inzicht in wie dat gebruikt voor welke doeleinden. Controle en inzicht hebben. Denk natuurlijk ook aan het idee dat je zelf je data kan manipuleren en verwijderen en veranderen etc. Dat heeft te maken dat we bij Sense niet zozeer alleen zien als een objectieve waarheid, maar als je je eigen context gaat verzamelen. Je gebruikt het als persoon om je eigen toestand te kunnen communiceren met anderen. Wat jij communiceert met anderen is je eigen gelegenheid. Als er wat anders naar de wereld gecommuniceerd moet worden dan wat er is waargenomen, dan moet je dat natuurlijk zelf weten. Plus wat telt is dat niet zomaar iemand bij je data moet kunnen, dus beveiligingsaspecten en dat soort zaken zijn altijd belangrijk. Het is een feit dat we daar natuurlijk ook proberen in de projecten zo lang mogelijk vol te houden. Dus bij PsyQ kwam de vraag of we de gegevens die met Sense verzameld werden ook voor onderzoeksdoeleinden mochten gebruiken. Dat kan, maar dat moet je vragen aan de patiënten. Die moeten toestemming geven. We zullen het meenemen in de vragen van de mensen die meedoen. Van ons mag het wel, maar ik heb niks te zeggen over die data. De techniek kun je zo inrichten als je wilt, wij bieden de tools om het op die manier te kunnen, dan heb je op die manier de filosofie gemaakt, maar we proberen het ook bij eindgebruikers en bij klanten zo in te zetten. Meestal snappen ze het dan ook wel. De neiging is toch te gaan doen en de data wel te gebruiken.

I: Omdat het waarschijnlijk ook een stukje gemakzucht is?

R: Mensen denken vanuit hun eigen positie en niet vanuit mensen.

I: En als je al die mensen moet vragen mag ik jou data en jou data, dan kost dat waarschijnlijk meer moeite dan hier heb je alle data?

R: Ook dat, maar mensen denken ook op de een of andere manier dat de data van hun is, omdat zij misschien alleen het systeem gemaakt hebben waarmee het verzameld wordt.

I: Of omdat zij de baas zijn van het bedrijf?

R: Of omdat zij daar de baas van zijn etc. dus niet alleen gemakzucht. Misschien is dat wel het laatste. Het gemakzucht schuiven ze wel op ons af: regelen jullie dat?

I: De hoeveelheid data die voor mensen wordt verzameld ...Voor toepassingen, stel je hebt een toepassing waarbij je wilt bijhouden waar iemand is en in de Sense app wordt alle sensordata eruit getrokken – uit de telefoon die je kan vinden van iemand, omdat dat misschien kan bijdragen aan het weten waar iemand is. In hoeverre is dat een probleem? Dat je eigenlijk meer data verzameld dan nodig is.

R: Dat ligt eraan of de gebruiker dat een probleem vindt. Je kunt natuurlijk kiezen welke sensoren je aan zet en welke je afsluit. Op individueel niveau kun je best wel veel informatie van jezelf verzamelen als je maar selectief kan zijn in wat je deelt. Je kunt natuurlijk in Sense de ruwe sensordata voor jezelf houden en de geïnterpreteerde waarden, zoals alleen waar je bent, kun je delen. Dat is iets wat, die slag zit vaak niet in andere systemen. Daar worden alle ruwe data in een bak gegooid. Maar goed, dat is een keuze, want je kunt natuurlijk ook zeggen 'gooi maar alles weg wat je niet nodig hebt', dat zou je als gebruiker kunnen zeggen. Weggooien is ook een aangelegenheid van de gebruiker. Zowel verzamelen als weggooien. Dus ik kan niet beslissen of iets te veel of te weinig data is.

I: Waar denk jij dat gebruikers zich uiteindelijk druk om zouden maken als ze Sense zouden gebruiken?

R: Batterij gebruik.

I: En met betrekking tot privacy?

R: Ik denk dat er een heleboel mensen zijn die zich daar helemaal niet druk om maken. Zelf doe ik dat ook niet echt. Of omdat ik weet wat er speelt, toch heb ik er niet zoveel moeite mee als Google mijn mails kent om mij aanbiedingen te doen. Op de een of andere manier heb ik er niet



zoveel last van. Als er een direct voordeel is, zijn mensen heel snel bereid data te delen of privacy op te geven. Er zullen altijd een paar die-hard's zijn die meningen heel erg kunnen beïnvloeden, de activisten van het internet zeg maar. Die zullen heel kritisch zijn, met name op beveiliging, maar ook of er niet een soort verborgen agenda is om wat anders met die data te doen. Dat los je op door transparant te zijn over wat je met de data gaat doen. Maar ook om vanuit Sense te vragen of je wat met de data mag gaan doen of niet. Op het moment dat je ze een voorbeeld laat zien hoe je de data wel gebruikt, maar dat dat alleen kan als je dat deelt, dan geeft dat misschien vertrouwen dat er op de achtergrond niks anders gedaan wordt. Als je helemaal niks doet met de data, worden mensen achterdochtig.

I: Ah ok, je zegt van 'je zou eigenlijk iets met de gebruikersdata moeten willen doen'

R: En ze dan vragen of het principe duidelijk is, dat dat ook voor ons geldt om de schade te beperken. Los van dat ze zich zorgen maken, moet je dat ook echt doen. Niet stiekem zoals TomTom toch de data gebruikt om de politie te helpen flitspalen ter plaatsen.

I: Dan worden mensen daar toch minder gelukkig van.

R: Zeker omdat ze hun TomTom er niet voor aanschaffen.

I: Welke van de partijen die jij hier in je netwerk hebt gezet. Denk je dat er stukken zijn die heel anders over privacy denken dan hoe jij er over denkt? Of een beetje anders, mag ook.

R: Jahoor, er zijn zeker partijen die er anders over denken.

I: Welke dan?

R: Nouja, dat gaat zowel om de visie op privacy als de implementatie ervan. Wat je bij developers en eindgebruikers vaak hoort is dat ze de cloud niet accepteren. Ze willen een privé-infrastructuur, zodat ze zeker weten dat die data niet buiten...het cloudaspect valt in veel bedrijven niet in hele goede aarde. In health care zie je dat de eisen nog veel strenger zijn: persoonsgegevens en medische data mogen niet op een systeem. Dat is eigenlijk nog veel strenger dan dat wij in principe voor ogen hadden. Vaak zie je dat ziekenhuizen daar ook niet heel erg rationeel in zijn, maar een soort 'cover-your-ass'-procedure hanteren. Opzich is dat wel goed, maar dat zie je. Ik denk dat dat er bij sommige partners en bij sommige klanten de wens leeft om de data te gebruiken, ook al is die van eigen gebruikers. Daar is natuurlijk ook de frictie 'kunnen wij de data niet gebruiken'.

I: Het gaat eigenlijk om de developersfractie die tussen de eindgebruikers en Sense zitten.

R: Partner zijn kun je zo zien. Maar eindgebruikers ook. Er komt ook veel commentaar van eindgebruikers vandaan. Als je kijkt naar mensen hier binnen het bedrijf dan denk je dat die wel redelijk gelijk denken over privacy. Als je kijkt naar gemeenschappen waarbinnen wij ons verhaal vertellen, denk ik dat daar nogal verschillen in zitten.

I: Welke sectoren zijn er dan vooral anders.

R: Als je dan bijvoorbeeld kijkt naar beveiligingsbedrijven. Die zijn niet gewend om vanuit gebruikers te denken, die denken vanuit de situatie. Je ziet in verschillende gemeenschappen verschillende standaarden hoe erg privacy is. Dat hangt van de omgeving af. Als je kijkt naar de concurrentie, laten we onderaan beginnen, custom solution, die denken niet zo na over privacy. Daar staat de klant centraal en niet zozeer de gebruikers. In context aware apps is het wel beter denk ik, daar is het vaak wat meer in generieke zin open. Hetzelfde geldt eigenlijk voor veel van die internet of things platformen: of het is een gesloten platform, maar dan is de data ook beschikbaar voor degene van wie dat platform is voor allerlei doeleinden. Of het is een open platform waarin je per definitie alles publiceert. Je hebt vaak weinig mogelijkheid tot nuance of gradaties waarin je iets deelt of niet deelt.

I: De keuze ligt eigenlijk ook niet bij de gebruiker zelf op het moment dat hij gekozen heeft voor dat platform.

R: Vaak kun je hem ook nog wel dichtzetten. Cosm is vaak bedoeld om een soort YouTube te zijn voor sensordata. Dat betekent dat je het als het ware de wereld in gooit. Mensen kunnen daarmee doen wat ze willen. Daar heb je ook weer gesloten groepen, dat zijn echter allemaal meer uitzonderingen dan dat het fundamenteel erin zit. Als je kijkt naar zoiets als 4Home, voor domotica, dat wordt door Ferizon in Amerika uitgerold. Daar wordt geagreggeerde data ook wel gebruikt voor marketing doeleinden. Daar heb jij niet zoveel meer over data te zeggen. Eigenlijk hetzelfde als wat telecomproviders ook doen, die proberen eigenlijk zoveel mogelijk te snappen en ze zeggen "al het verkeer wat over onze infrastructuur rijdt monitoren wij en dat mogen wij."

I: Maar jij zegt bij Sense zeggen we dat het niet onze data is, dus daar mogen we niet zomaar

ongevraagd wat mee doen?

R: De essentie is heel sterk dat wij niet een platformperspectief hebben maar een gebruikersperspectief en dat heeft consequenties. En in sommige gevallen zijn we daardoor minder open en in andere gevallen opener. In sommige gevallen gaan we zorgvuldiger met data om dan in andere gevallen.

I: Kun je daar voorbeelden van geven?

R: Dat heb ik net gedaan.

I: Ja. Dat is waar. Ik dacht 'misschien heb je nog meer'.

R: Als je kijkt naar een home-automation waarbij je data standaard gebruikt wordt door zo'n partij om te snappen hoe of wat, dan zijn wij minder open. Als je kijkt naar een platform wat alles maar publiceert, zijn wij natuurlijk geslotener.

[33:00]

I: Ok. Hoe denk jij dat het in de producten van Sense zelf zit qua hoe jij denkt over privacy? En ook implementatie daarvan? Zit daar verschil tussen?

R: Ja, we zijn niet zover als ik zou willen, maar dat is een kwestie van effort en tijd, in termen van transparantie naar de gebruiker toe. In de termen van hoe visualiseer je en hoe geef je ze daar nog betere control over. In termen van dat die controle technisch gezien wel heeft en dat je als gebruiker moet bepalen of je iets wilt of niet. Dat wordt dus eigenlijk ook automatisch aangemaakt, maar dan zit het hem ook in de communicatie met de gebruiker. Bijvoorbeeld een TNT-chauffeur, als je die app download en je logt in, dan gaat 'ie automatisch jouw GPS-locatie delen met je baas. Dat hoeft je niet expliciet aan te vinken, maar eigenlijk accepteer je dat wanneer je die TNT-app download. Dus heel veel is ook 'je hoeft niet alles in te stellen, als je het maar als geheel regelt.' Daar wordt het natuurlijk al wat diffuser, daar helpt het als je het wat meer inzichtelijk maakt. Ik denk dat dat de inzichtelijkheid en transparantie vergroot. En daar kan nog wel wat gebeuren. In de basis zijn de projecten redelijk overeenkomend met dat wat we daarvan vinden. Goed er is nog werk te verzetten.

I: Er is nog werk te verzetten. Wat jou betreft vooral op transparantie gebied?

R: Ja. Ik denk dat we nog actiever bezig kunnen. Er ontstaat nu wereldwijd een grote community die over dit soort dingen nadenken, die ook proberen om tot een soort moreel stuk te komen waarmee we bezig waren.

I: Hoe heet die club?

R: Dat zal ik even voor je opzoeken.

I: Vooral omdat jij hebt aangegeven 'we willen graag ons standpunt naar de wereld brengen'.

R: Ja. De open-internet-of-things-assembly. The first annual open IOT-assembly. Assembly is a gathering of people who took strong primacy of control of IOT-services. Het komt uit een van de concurrenten. En die hebben een IOT-assembly georganiseerd. Dat is iets waar wij ons ook bij zouden moeten aansluiten.

I: Ja, om dat zelf op te zetten is een beetje dubbelop.

R: Nu wel.

I: Als je een jaar eerder was geweest.

R: Precies.

## Covenant

I: Dan nog een vraag die al een beetje in de andere vragen zat, maar ik ga hem toch stellen. Stel jij zou Sense zijn, wat zou je dan aan de wereld willen beloven met betrekking tot privacy?

R: Stel ik zou Sense zijn? Dat vind ik een hele rare...

I: Stel jij bent het bedrijf Sense, jij representeert dat en jij beslist wat Sense gaat beloven aan de wereld.

R: Stel...

I: Puur hypothetisch. Bij anderen is het misschien meer hypothetisch

R: Hypothetisch. Ik denk net de visie die ik net genoemd heb.

I: Wat je net genoemd hebt.

R: Ja.

I: En dan nog de samenvattende vraag. Wat moet er vooral nog gebeuren om te zorgen dat dat ook echt zo gaat zijn? Dat je die belofte waar kan maken.

R: Een is transparantie wat ik al noemde. Twee is communicatie erover. Drie is toch ook het

advies kunnen geven over een project als geheel vanuit basiswaarden. Het hoeft niet altijd technologisch te worden opgelost, maar ook in communicatie naar eindgebruikers. Het kan best zijn, waarom zou je alle vinkjes moeten laten aan zetten omdat hij TNT-chauffeur is en met privacy te maken heeft. Het gaat om transparantie binnen het hele traject. Daar wil je per traject een idee over krijgen. Niet alleen specifiek in het gedeelte van Sense. Daar hoeft niet altijd de oplossing te zitten, het kan ook ergens anders zitten. Dat is iets wat we moeten doen om dat goed voor elkaar te krijgen. Hoe dat er precies uit zit weet ik niet. De basiswaarde is het in ieder geval een paar keer doorlopen hoe dat dan in bepaalde projecten zit. Voorbeeldcases. Het zou ook best kunnen zijn dat je daar zelf een bepaalde visie over hebt of een bepaald onafhankelijk orgaan die dat aanpakt. Privacy-proof ofzo. Safety-proof. Dat je gecertificeerd bent ofzo.

[40:08]

I: Hoe zit het daar eigenlijk mee? Tijdens die meeting over het document, zei je, had je het over een aantal certificaten. Een voor de zorg en een voor de privacy in het algemeen.

R: Ja, NEN7510 en ISO27001.

I: Wordt daar actief naartoe gewerkt? Want je zei, het zou wel gaaf zijn als we dat kregen.

R: Dat is een typisch geval van cross the bridge when you get there . Het is een noodzakelijke voorwaarde, daar zitten veel andere dingen omheen qua standaardisatie, het is voor 50% nuttig en voor 50% een barri re of entry, die grote partijen vaak opzetten zodanig dat die markt een beetje controleerbaar blijft. Er spelen allerlei dingen een rol. Wat mij betreft, we zitten nu in een fase waarin innervatie werkend moeten krijgen. De volgende stap is om voor een bepaalde markt de nodige certificeringen te halen. Die zijn in alle markten weer anders en bij ieder vereiste heb je weer een soort partner die daarin helpt. Het feit dat er ook een soort IOT-assembly nodig is, is dat dat ook nog in ontwikkeling is, daar zijn zeker nog geen standaard procedures voor. De dingen die er al zijn zijn toch al meer standaard en komen uit een andere groep. Daar moet je aan voldoen om bepaalde dingen te mogen leveren in verschillende markten. Dat zijn voorwaarden. Die zijn per markt anders. Je moet per markt kijken hoe je dat voor elkaar krijgt en of je daar partners bij nodig hebt. Dat is niet iets waar we voorlopig al mee aan de slag zijn, wat mij betreft. En zeker als klein bedrijf moet je dat gewoon zo lang mogelijk uit stellen. Het kost klauwen met geld en levert eigenlijk niks op. Pas op het moment dat het een probleem wordt, moet je het oplossen.

I: Je zegt ook, we moeten aan die transparantie gaan werken.

R: In een generiek platform moet je dus fundamentele principes goed hebben en je moet de tooling hebben om dingen te kunnen vormgeven en vervolgens moet je per markt de toepassing zo laten vormgeven dat je het kan toepassen in die markt.

I: Even kijken. Volgensmij hebben we hem bijna gehad. Ik ben toch nog benieuwd, dingen als de website en andere communicatiemiddelen waar jij als Sense je boodschap naar buiten brengt, komt daar de boodschap over privacy ook naar voren?

R: Op sommige pagina's wel, maar representatief niet. Te weinig. Nee, zoals ik ook nu met jou zit te praten, hoe ik ook met anderen praat of als ik praatjes geef, de manier waarop ik dat probeer te verwoorden vindt iedereen wel erg prettig, daar zijn ze het dan wel mee eens, maar dat kun je op de website niet terugvinden of in de documentatie die je in commonsense hebt. Dus te weinig, ja.

I: Databeveiliging. Dat hangt ook samen met of je mensen hun gegevens goed kan laten afschermen. In hoeverre is dat een ding waar nog heel veel aan gewerkt moet worden of iets waar Sense anders over denkt dan de rest van de wereld?

R: Ik denk dat het in de basis goed geregeld is. Afscherming met een password. Het is nu wel zo dat de data zelf niet nogmaals in incripten wordt opgeslagen als ik het goed heb, dus dat betekent dat het systeem beveiligd is. Je wachtwoorden in plain text opslaan, zo erg is het bij ons dan ook nog niet, dat gebeurt ook nog, maar de data zelf is niet incripted en de vraag is of dat moet en of je dat wil. Waar ik over moet nadenken is hoe je ook nog de correlatie tussen data op de een of andere manier kunt verbergen en dat is natuurlijk niet triviaal. Dus bijvoorbeeld als ik weet dat jij op een bepaald moment ergens was en ik ga door die data heen zoeken wie er allemaal op dat moment op die plak waren kan ik vervolgens daar ergens een lijntje trekken en kan ik toch nog een heleboel data terugvinden van jou. Dat is iets wat we nog niet hebben opgelost, denk ik, maar dat is triviaal. Dat is wel heel veel stappen vooruit gedacht hoe je dat doet. Daar moet nog meer aan gebeuren. Maar in de basis is de databeveiliging redelijk uniform.

I: Dat waren eigenlijk wel de vragen. Heb jij nog dingen toe te voegen die je graag kwijt wilt en

die meegenomen moeten worden als het over privacy gaat?

R: Wanneer is het document af?

I: Het document van STAFF4 ...dat is een goeie. Daar moet ik ook nog even naar zitten. Kan ik volgende week even naar kijken.

R: Ik heb niks meer. Ben jij tevreden met mijn input?

I: Ik ben prima tevreden. Vooral het stukje transparantie komt in veel interviews naar voren. Dat is mooi dat daar overeenstemming in te vinden is. Ik heb nog geen grote crisis binnen het bedrijf weten vast te stellen.

R: Ik ben benieuwd wat STAFF2 ervan gaat vinden. Niet zozeer omdat ik bang ben wat STAFF2 ervan vindt, maar vooral omdat STAFF2 er wat verder vanaf zit. Dan is de kans dat dat wat verder uit elkaar ligt groter. Maar laten we wel zijn, convergentie van ideeën is evenredig met de communicatiefrequentie. Dat is dan weer een mooi onderwerp voor een promotieonderzoek. Als je gewoon maar communicatiepatronen in kaart brengt dan kun je ideeën ook wel zien.

I: Aan de hand van hoe vaak mensen met elkaar hebben over dingen kun je wel zeggen dat die overeen komen?

R: Als wij het dagelijks over dit soort dingen hebben, dan kun je er donder op zeggen dat, dat is ook het doel convergeren, het doel van een gesprek, dan kun je ook zeggen we hebben sowieso een goede verstandhouding, gesprek alleen is niet voldoende, er moet ook inhoud zijn. Maar als je hierover regelmatig praat met elkaar dan moet dat tot convergentie leiden. Maar het kan ook de verkeerde kant op gaan, daarom moet je er ook nog met anderen over praten.

I: Dat ligt eraan wat je de verkeerde kant vindt.

R: Als je met z'n alleen een kant op convergeert zonder dat je daar andere stake holders erbij betrekt. Dan ga je misschien ergens een hoek in waar je niet heen wilt.

I: Ik was afgelopen week naar een paar mensen geweest die het model met welke stake holders je waar in kaart moet brengen, die dat hadden gemaakt en een boek geschreven hebben. Die zeiden: misschien is het voor je interviews relevant om toch drie externe stake holders te interviewen om te vragen wat die erover denken dus dat moet ik als ik het netwerkplaatje bij elkaar heb gevoegd even bekijken.

R: Daar kom je op veel meer verschillen als dat je alleen intern gaat kijken.

I: Ik denk alleen niet dat die het hele netwerk hoeven te tekenen vanuit hun. Dat is wat minder relevant voor Sense.

R: Of betrokkenen gegeven de samenwerking met Sense. Je kan in ieder geval – als je ze toch opzoekt, kun je ze meteen naar mij sturen – een samenvatting van de Internet of Things assembly dat is ook meteen input. Dat hoef je niet te vragen, dat gaat in notulen. Want die hebben het precies hierover. Dat is hun antwoord op deze vragen. Moet je hier nog een foto van maken?

I: Ja, daar moet ik nog een foto van maken. Dankjewel.

R: Alsjeblieft.

## C.8. Staff 4

Of this respondent, no video was recorded. However, the information presented in the summary below has been checked and approved by the respondent.

### Network

Het netwerk is als tekening op een losse foto opgeslagen. Begeleidende tekst is als volgt: De relatie met andere medewerkers is dusdanig dat STAFF3 uiteindelijk het einddoel bepaald met betrekking tot beleid. Met betrekking tot de toepassingen van Sense houdt STAFF4 zich vooral bezig met de marketing/verkoop kant. De teksten over CommonSense op de website zijn ondertussen 1.5 jaar oud en niet altijd meer geldig. Pas als de applicaties voltooid zijn komt STAFF4 in het spel. Dit vanwege haar rol in de marketing/verkoop. Ze heeft niet veel contact met klanten, dit gaat vaak in eerste instantie via STAFF3 of STAFF2. De inhoud van de website heeft ze in combinatie met Rotterdam CS (de website-host en zuster van Sense) opgezet. Veel Almende-producten bevatten Sense-technologie, waardoor andere zusterondernemingen als klant/partner van Sense optreden. Concurrenten van Sense zijn bijvoorbeeld Patchbay, die voornamelijk publieke sensoren delen. Andere concurrenten heeft STAFF3 meer verstand van, hij houdt dit bij. Communicatie met de pers is een manier om de visie van Sense met de wereld te delen.

### Privacy

Privacy volgens STAFF4 is het recht of de mogelijkheid om zelf te bepalen wie wat over jou te weten kan komen. STAFF4's angst op het gebied van privacy gaat over secondary use. Dit gaat over het doorspelen van haar informatie door andere partijen. Ook met betrekking tot gegevens die je niet kan afschermen, zoals de gegevens bij banken en overheden. Koppelen van data van verschillende bronnen die individueel niet gevaarlijk lijken is ook een issue. Ze geeft als voorbeelden mashups tussen foursquare en facebook waarbij bars waar veel vrouwen zijn gevonden kunnen worden.

### Covenant

Als STAFF4 zelf de merkblofte van Sense zou mogen neerzetten, zou er duidelijk gemaakt worden dat de data afgeschermd is, en zou ze ook graag de mogelijkheid bieden dit te controleren. Ook het feit dat Sense medewerkers zelf niet bij de data kunnen is belangrijk om mee te delen. Met wie je de data deelt is je eigen verantwoordelijkheid, maar gebruikers mogen wel onderwezen worden over hoe er verantwoordelijk met data omgegaan kan worden.

### Analysis

Over de strategie van Sense weet STAFF4 te zeggen dat de visie er wel is, maar de praktijk blijft achter. De strategie en visie met betrekking tot privacybeleid bestaat al 2-3 jaar (sinds dat Sense bestaat), maar in implementatie ontbreekt het nog. Tussen de visie van het topmanagement en strategie ziet ze weinig verschil (Ideal en Desired Identity). De visie van STAFF3 met betrekking tot eigendom van data is gelijk aan die van STAFF2 (directeur Almende). In de visie van bedrijven in de Almende-group speelt zelforganisatie een belangrijke rol, wat leidt tot verantwoordelijkheid en eigendom van data bij de eindgebruiker (bottom-up ipv top-down) De externe partijen waar Sense nu mee samenwerkt gaan vaak nog uit van een top-down visie. De medische partners zien niet in dat de patient eigenaar van zijn eigen data is. De bedrijven in de kassenbranche zouden wellicht positiever staan tegenover het loslaten van de data van anderen. Over het algemeen echter, hebben partnerbedrijven vaak weinig boodschap aan het idee dat data eigendom is van de maker er van. STAFF4 ziet wel een kans in de trend dat eindgebruikers langzaam beseft krijgen dat data waardevol en persoonlijk eigendom is. Hier ligt volgens STAFF4 een B2B-kans voor Sense om voorbeeld op dit gebied te zijn.



# D

## Labelled actor lists

This chapter summarizes the information obtained from the transcribed interviews in appendix C. These summaries are an interpretation showing how the interview responses map onto the privacy aspects summarized in section 4.3.10. The tables in this chapter use short form notation of both the networked identity types and the principles of fair information practices. For identity types, the following notation is used:

**Pers** subdivision personnel of the Actual identity

**Prod** subdivision products of the Actual identity

**Com** Communicated

**Con** Conceived

**Id** Ideal

**Des** Desired

**Cov** Covenanted

The principles of fair information practices are indicated by:

**O&T** openness and transparency

**IP** individual participation

**CL** collection limitation

**DQ** data quality

**UL** use limitation

**RS** reasonable security

**Ac** accountability

**IO** individual ownership

**CAD** complete access denial

! indicates contradiction of the term behind this sign

## D.1. Developer 1

Intermediary	Identity Type(s)	Privacy Principle(s)
DEV1 DEV3 DEV4 STAFF3	Pers & Id & Des Pers & Id & Des Pers & Id & Des Pers & Id & Des	UL, CAD adheres to covenant adheres to covenant adheres to covenant
MiriaNed CommonSense API	Prod Prod Prod	UL, !CAD, !IO UL, !CAD, !IO
DevLab-dag STAFF4 publicaties nieuwsberichten automatiseringsbladen Sense website	Com Com Com Com Com Com	!O&T
Martin (GreenFormula) Lex (DevLab) Hogeschool Rotterdam Almende Vitelec Worm Chess HRo GreenFormula	Com & Con Com & Con Com & Con Con Con Con Con Con Con	[see staff-2] O&T IO
DevLab Zorg Glastuinbouw Let's grow Kosm	Con & Id Con & Id Con & Id Id Id	RS UL, RS UL, RS UL !UL
STAFF2	Id & Des	
Covenant	Cov	UL, IP, RS, IO



## D.2. Developer 2

Intermediary	Identity Type(s)	Privacy Principle(s)
DEV2 DEV4 DEV3 STAFF3	Pers Pers Pers Pers & Com & Id &	UL, IO, O&T, RS, !CAD, Acc
Back-end Sense App activity tracker iVitality indoor localisation Simon Sense	Prod Prod Prod Prod Prod Prod	!O&T, !RS, !CAD, !Acc !O&T, !RS, !CAD, !Acc !UL !UL, !CAD
pulseTracks gebruikers iemo Almende AliensAreAmongUs	Con Con Con Con Con	!UL & O&T !UL
Skype meetings appStore website	Com Com Com	!O&T
FitBit MapMy Concurrenten Google Almende DevLab jaarlijkse bijeenkomst technologie	Id Id Id Id Id Id Id Id	
STAFF2	Id & Des	
Covenant	Cov	O&T, UL, IO, CAD

### D.3. Developer 3

Intermediary	Identity Type(s)	Privacy Principle(s)
DEV3 STAFF3 DEV4 DEV2	Pers, Comm, Id, Des Pers, Comm, Id, Des Pers, Id, Des Pers, Id, Des	UL, !CAD
CommonSense Sense App Dashboard 3rd party apps iVitality Moodie Paige DEAL	Prod Prod Prod Prod Prod Prod Prod Prod	UL, !CAD, !RS, !O&T UL, !CAD, !RS, !O&T O&T !O&T !O&T, UL
demos presentaties developer forum vaktijdschriften beurzen	Com Com Com Com Com	UL UL UL UL UL
Hogeschool Rotterdam Almende Ask Deal Almende ATUS security Commit P3	Com & Con Con Con Con Con Con Con	
STAFF2 LUMC Parnassia OpenSense Kosm (former Pachube)	Id Con & Id Con & Id Id Id	
Covenant	Cov	UL, RS, CAD

## D.4. Developer 4

Intermediary	Identity Type(s)	Privacy Principle(s)
DEV4 DEV5 DEV3 DEV2 STAFF3	Pers & (Id) Pers & (Id) Pers & (Id) Pers & (Id) Pers & Com & Id & Des	UL, O&T, IP, IO
backend CommonSense dataopslag (PHP, MySQL, MongoDB) API data processing 3rd party apps	Prod Prod Prod Prod Prod	UL, IP, !O&T, !RS, !CAD UL, IP, !O&T, !RS, !CAD UL, IP, !O&T, !RS, !CAD UL, IP, !O&T, !RS UL, IP, !O&T !UL
evenementen onderzoek netwerkbijeenkomst sensors directe chat Dag van de Zelforganisatie	Com Com Com Com Com	
3rd party developers DevLab Almende Ask Deal DO	Con Con Con Con Con Con	UL, O&T, IP UL, O&T, IP UL, O&T, IP UL, O&T, IP
Dysi Google Cosm STAFF2	Id Id Id Id & Des	RS, UL
Covenant	Cov	RS, UL

## D.5. Staff 1

Intermediary	Identity Type(s)	Privacy Principle(s)
STAFF1 STAFF3 DEV2 DEV1 Stagiairs Medewerkers	Pers Pers & Com Pers Pers Pers Pers & Id	UL, CL, Ac,
Producten Indoor localisatie	Prod Prod	!CAD
stagemarkt website bellen mailen post	Com Com Com Com Com	
Almende	Con & Id	
Zorg en welzijn Sport Het nieuwe werken	Id Id Id	UL, RS !UL
STAFF2	Id & Des	
Covenant	Cov	UL, RS, O&T

## D.6. Staff 2

Intermediary	Identity Type(s)	Privacy Principle(s)
STAFF3 DEV3 DEV1	Pers & Id & Des Pers Pers	
Sense App Sense Platform Sense halffabrikaat	Prod Prod Prod	!RS, !CAD !RS, !CAD !RS, !CAD
Website Rotterdam CS STAFF4		
iVitality Parnassia MentalShare Ask Deal Do Jansen Sinach	Con Con Con Con Con Con Con	RS, !IO RS, !IO RS, !IO
OpenSense Pachube (Cosm)	Id Id	
STAFF2	Des	IO, IP, UL, RS, CAD
Covenant	Cov	IO, RS, UL, CAD

**D.7. Staff 3**

Intermediary	Identity Type(s)	Privacy Principle(s)
DEV1 DEV3 STAFF3 STAFF1	Pers & Id & Des Pers & Id & Des Pers & Id & Des Pers & Id & Des	O&T, IO, IP, UL, RS
CommonSense Dashboard	Prod Prod	UL, !O&T, !RS UL, !O&T
STAFF4 Website beurzen praatjes conferenties magazines weblogs filmpjes	Pers Com Com Com Com Com Com	!O&T O&T
Almende R&D Ask, Deal, Do DevLab Chess GreenFormula Partners Beslissers (eind)gebruikers	Con Con Con Con Con Con Con Con Con	!UL !UL
Cosm OpenSense Context aware apps Custom solutions Internet of Things concurrentie market opportunities development roadmap dochters beschikbare tools technology environment Healthcare Logistics Security	Id Id Id Id Id Id Id Id Id Id Id Id Id	!UL !UL !O&T, !UL !IP, !IO !IP
STAFF2	Id & Des	
Covenant	Cov	O&T, IP, UL, RS

**D.8. Staff 4**

Intermediary	Identity Type(s)	Privacy Principle(s)
STAFF3 STAFF1 Roelof	Pers & Id & Des Pers Pers	
CommonSense Apps	Prod Prod	
STAFF4 Website (vak) pers	Com Com Com	UL
site-bezoekers Rotterdam CS Ask Deal Pachube Healthcare	Con Con Con Con Con Con	!IO
STAFF2	Id & Des	
Covenant	Cov	O&T, RS, CAD

# Glossary

## Sense

The software company [Sense Observation Systems](#) (Sense), a daughter of [Almende](#), based in Rotterdam, The Netherlands. The company develops context aware applications for smartphones; their software monitors the activities of the user, and helps provide this user with personalized coaching, or advice.

## Privacy

This research focuses on *information privacy*, which concerns access to individually identifiable personal information, and is part of the concept of *general privacy*. From the field of Information Systems Research, we use the generally accepted [26] definition by Westin [33] to define *information privacy* as:

“the ability of individuals to control the terms under which their personal information is acquired and used”

## Privacy aspects

The concept of *information privacy* is operationalized using the Concern For Information Privacy-scale by Smith et al. [25], the Principles of Fair Information Practice by Westin [33], and the responses obtained during the interviews. This operationalisation resulted in a set of aspects related to *information privacy* considered relevant for the business of Sense. The elaborate definitions of these aspects can be found in section 4.3.10, whereas the compact summary of the aspects is seen in table 4.1, which also shows how the different aspects are represented visually throughout the thesis.

## Identity

The *identity* of a company, defined by all stakeholders involved in the company. We research the identity by looking at different *identity types*.

## Identity types

Based upon the AC<sup>3</sup>ID-model by Balmer and Greyser [2], and the apparent difference [18] between employees and products in implementation of *privacy* aspects, we define 7 distinct identity types:

- Personnel Identity, part of the Actual Identity in Balmer and Greyser [2]
- Product Identity, part of the Actual Identity in Balmer and Greyser [2]
- Communicated Identity
- Conceived Identity
- Ideal Identity
- Desired Identity
- Brand Identity, known as Covenanted Identity in Balmer and Greyser [2].

## Actor

Actors are defined as humans or objects capable of interacting with one another (exchanging beliefs). This interaction can be either direct, or through the use of *intermediaries* (objects or meetings that do not themselves initiate interaction).

## Network

With this term we mean the set of *actors* that have a direct influence on one of the *identity-types* related to the *Sense*. This network includes all external stakeholders. The set of *actors* is defined through the interviews in section 4.4.

**Actor cluster**

A group of *actors* which fall within one *identity type* who value similar *privacy aspects*. During the exploration of *identity types* (section 4.4), these *clusters* are defined through the action of punctualisation. Based on the interviews, we define the actor clusters found in table 4.9. The brand identity does not contain any *clusters*, because this is the *identity type* for which a fitting *aspect* is sought. Per *identity type*, we define the following:

**Personnel** extensive, selective

**Product** old, new

**Communicated** media

**Conceived** Almende, health, sports

**Ideal** market

**Desired** vision

**Privacy landscape**

A visualisation of the *actor clusters* in relation to one of the *privacy aspects*, used to visualize points of attention for making that *privacy aspect* central to the identity of *Sense*.



# Bibliography

- [1] S. Albert and D. A. Whetten. Organizational Identity. *Research In Organizational Behavior*, 7(1):263–295, 1985. ISSN 01913085.
- [2] J. M. Balmer and S. A. Greyser. Corporate marketing: Integrating corporate identity, corporate branding, corporate communications, corporate image and corporate reputation. *European Journal of Marketing*, 40(7/8):730–741, Jan. 2006. ISSN 0309-0566. doi: 10.1108/03090560610669964.
- [3] J. M. T. Balmer and S. A. Greyser. Managing the multiple identities of the corporation. *California Management Review*, pages 71 – 86, 2002.
- [4] M. Callon. Techno-economic networks and irreversibility. In J. Law, editor, *A Sociology of monsters essays on power technology and domination*, volume 38, pages 132 – 161. Routledge, New York, New York, USA, 1991. ISBN 0415071399.
- [5] A. Collins, D. Joseph, and K. Bielaczyc. Design Research: Theoretical and Methodological Issues, 2004. ISSN 1050-8406.
- [6] M. J. Culnan and R. J. Bies. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2):323–342, 2003.
- [7] European Commision. Protection of personal data, 2014. URL <http://ec.europa.eu/justice/data-protection/>.
- [8] M. E. Falagas, E. I. Pitsouni, G. A. Malietzis, and G. Pappas. Comparison of PubMed, Scopus, Web of Science, and Google Scholar: strengths and weaknesses. *FASEB journal : official publication of the Federation of American Societies for Experimental Biology*, 22(2):338–42, Feb. 2008. ISSN 1530-6860. doi: 10.1096/fj.07-9492LSF.
- [9] G. Franzen and S. Moriarty. *The Science and Art of Branding*. M. E. Sharpe Incorporated, 2008. ISBN 9780765617910.
- [10] D. A. Gioia, M. Schultz, and K. G. Corley. ORGANIZATIONAL IDENTITY , IMAGE , AND ADAPTIVE INSTABILITY. *Academy of Management Review*, 25(1):63–81, 2000. ISSN 03637425. doi: 10.2307/259263.
- [11] R. Gross, A. Acquisti, and H. J. H. Iii. Information Revelation and Privacy in Online Social Networks ( The Facebook case ). *ACM Workshop on Privacy in the Electronic Society (WPES), 2005*, page 11, 2005. ISSN 15206106. doi: 10.1145/1102199.1102214.
- [12] R. Heersmink, J. den Hoven, N. J. Eck, and J. den Berg. Bibliometric mapping of computer and information ethics. *Ethics and Information Technology*, 13(3):241–249, Apr. 2011. ISSN 1388-1957. doi: 10.1007/s10676-011-9273-7.
- [13] T. Hoholm and F. H. Strø nen. Innovation, strategy and identity: a case study from the food industry. *European Journal of Innovation Management*, 14(3):345–363, Feb. 2011. ISSN 1460-1060. doi: 10.1108/14601061111148834.
- [14] G. Iachello and J. Hong. End-User Privacy in Human-Computer Interaction, 2007. ISSN 1551-3955.
- [15] M. Kilduff and D. J. Brass. Organizational Social Network Research: Core Ideas and Key Debates. *The Academy of Management Annals*, 4(1):317–357, 2010.

- [16] M. Kok and H. Barendrecht. *De zes kernen van een organisatie : een integrale visie op identiteitsmanagement*. Kluwer, Alphen aan den Rijn, 2011. ISBN 9789013081633.
- [17] K. Krukow, M. Nielsen, and V. Sassone. Trust models in ubiquitous computing. *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences*, 366(1881): 3781–3793, 2008.
- [18] S. Lahlou, M. Langheinrich, and C. Röcker. Privacy and trust issues with invisible computers. *Communications of the ACM*, 48(3):59, Mar. 2005. ISSN 00010782. doi: 10.1145/1047671.1047705.
- [19] M. Langheinrich. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In G. D. Abowd, B. Brumitt, and S. Shafer, editors, *Ubicomp 2001: Ubiquitous Computing*, volume 2201, pages 273–291. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001. ISBN 978-3-540-42614-1.
- [20] B. Latour. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press, 2005. ISBN 0199256047.
- [21] V. Luoma-aho and A. Paloviita. Actor-networking stakeholder theory for today’s corporate communications, 2010. ISSN 1356-3289.
- [22] M. Michael. *Constructing identities : the social, the nonhuman and change*. Sage, London; Thousand Oaks, Calif., 1996. ISBN 0803989512 9780803989511 0803989520 9780803989528.
- [23] P. A. Pavlou. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7(3): 101–134, 2003. ISSN 10864415. doi: 10.1.1.86.7139.
- [24] L. C. Schaupp, L. D. Carter, D. L. Schaupp, and N. C. A. Ethics in Social Networking: A Framework for Evaluating Online Information Disclosure. In *Proceedings of the 44th Hawaii International Conference on System Sciences HICSS*, pages 1–7, 2011. ISBN 978-1-4244-9618-1. doi: 10.1109/HICSS.2011.193.
- [25] H. J. Smith, S. J. Milberg, and S. J. Burke. Information Privacy: Measuring Individuals’ Concerns about Organizational Practices. *MIS Quarterly*, 20(2):167, June 1996. ISSN 02767783. doi: 10.2307/249477.
- [26] H. J. Smith, T. Dinev, and H. Xu. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4):989–1015, 2011. ISSN 15578607. doi: 10.1016/j.iac.2009.04.007.
- [27] M. Tassoul and J. Buijs. Clustering: An Essential Step from Diverging to Converging. *Creativity and Innovation Management*, 16(1):16–26, Mar. 2007. ISSN 0963-1690, 1467-8691. doi: 10.1111/j.1467-8691.2007.00413.x.
- [28] M. Tassoul and M. Houdijk. *Creative facilitation : a Delft approach*. VSSD, Delft, 2005. ISBN {907130146X} 9789071301469.
- [29] F. Thiesse. RFID, privacy and the perception of risk: A strategic framework. *Journal of Strategic Information Systems*, 16(2):214–232, 2007.
- [30] M. C. A. van der Sanden and F. J. Meijman. Evidence-Based Science Communication: An Essay. *Science Communication*, 25(3):272–287, Mar. 2004. ISSN 10755470. doi: 10.1177/1075547003262662.
- [31] R. R. R. van der Vorst. *Branding : a systems theoretic perspective*. Amsterdam, Oct. 2004. ISBN 9789090184357.
- [32] C. B. M. van Riel and C. J. Fombrun. *Essentials of corporate communication: implementing practices for effective reputation management*. Routledge, Abingdon, Oxon ;New York, NY, 2007. ISBN 9780203390931.

- 
- [33] A. F. Westin. *Privacy and Freedom*, volume 33. Atheneum, 1967. ISBN 0370013255. doi: 10.2307/2092293.
- [34] K. Wuyts, R. Scandariato, B. De Decker, and W. Joosen. Linking Privacy Solutions to Developer Goals. pages 847–852. IEEE, 2009. ISBN 978-1-4244-3572-2. doi: 10.1109/ARES.2009.51.