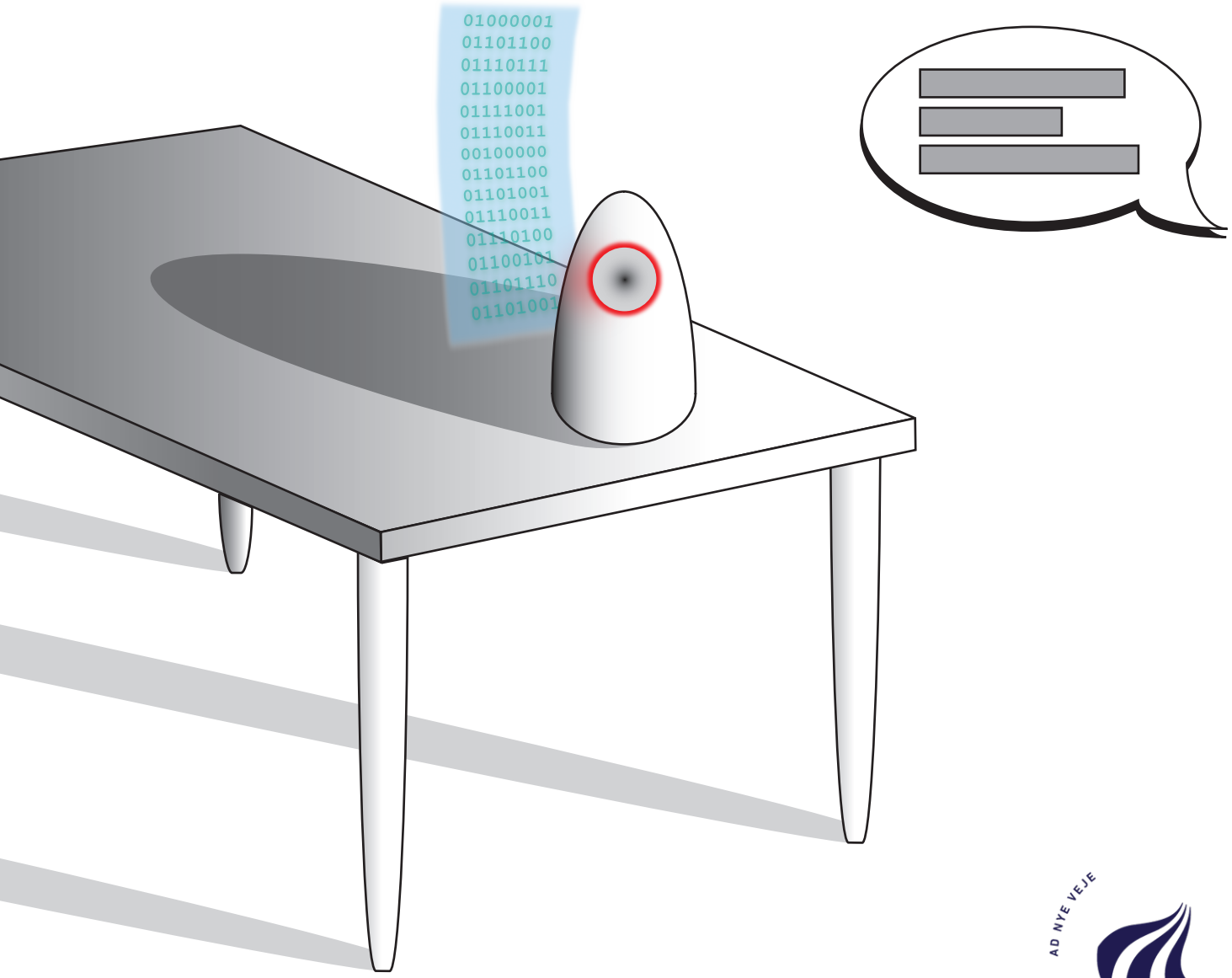
An assessment tool for evaluating users privacy perception of IoT-devices

Master's thesis
Engineering Psychology

Karolis Mikuta Nielsen



AD NYE VEJE
AALBORG UNIVERSITET

Title: An assessment tool for evaluating users privacy perception of IoT-devices
Semester: Master's Thesis
Project period: 06.02.20 til 04.06.20
ECTS: 30
Supervisor: Rodrigo Ordoñez

Karolis Mikuta Nielsen

SYNOPSIS:

This Master's thesis represents the work of developing a model for evaluating privacy perception for IoT-devices. The model was developed based on a comprehensive literature review and the main purpose was to compile dimensions for privacy perception to accommodate for the physical world. A subset of items have been found and modified to design a privacy perception scale (PPS). The PPS was used in an experimental set-up. The survey containing the experimental set-up was administered through different network fora. Respondents (N = 46) competed the survey and tested the questionnaire between two conditions. A PCA extraction compared by a parallel analysis found the model to only have one factor for the first condition and a EFA could not be made. This factor had a internally consistent of ($\alpha = 0.924$). A difference between privacy perception scale between the conditions was found ($r = .80$). In conclusion, the study found that the PPS can be used in order to assess the privacy perception of users of IoT devices.

Table of Contents

1 | Introduction

The implication of the internet has changed society and given rise to new ways of social interactions and communication. In the last years, new products have taken advantage of the internet by implicating it in devices like mobile phones, fridges, cars and toys. Such devices being interconnected by the internet are known as Internet of Things (IoT) devices. Often these devices are equipped with cameras, microphones and other sensors. The risk of privacy arises when information services collect personalized-user-behavioral-data whenever the device is active. This specific information can be gathered via normal usage of a service or indirect usage of a service. An example of information being gathered via normal usage is, when the user actively requests an action from a service. The information gathered is the action from the user and may be the answer given by the service. An example of indirect information gathering, can be at any occasion a device or web page is collecting information, but without the users‘ active interaction with of the service. A scenario for this could be a person that has her phone next to her and is talking to a person in the same room. While these two people are having a conversation, the phone could indirectly be gathering some sensory data of this interaction. The way the information could be collected, may in this scenario be, by recording the conservation with the microphone of the phone and thereby gathering audio data, which in turn could be transcribed into sensitive information. This practice is not exclusive to phones, but to every device or service that is connected to the internet and has at least one sensor. One of the reasons this data is collected is to personalize the experience when using a specific service. Even if people voluntarily give their information away without any consideration, missuses can occur and directly effect the individuals, if privacy is seen as trivial and not a concept that should be supported in the society. In order to prevent the missuse of the data obtained by IoT devices, privacy measures have been design. One example could be a cover in front of a camera sitting on the computer. It is questionable, how the user experiences its privacy with and without such privacy measures. As no assessment tool was found in the literature, the aim of this study is, therefore, to design a Privacy Perception Scale (PPS) for IoT devices that covers this physical component.

In the next section, a definition of privacy is obtained. The methodology to measure the privacy perception of IoT device users is then described. A PPS to measure the privacy perception of IoT device users is proposed and then tested by a within-study design containing two extreme scenarios. Lastly, the implication of the proposed PPS is discussed.

2 | Literature review

In the following chapter, the concept of privacy is explored. Moreover, it is investigated how the concept of privacy can be assessed in relation to IoT devices.

2.1 Background of Privacy

No single definition of privacy has gained universal acceptance [Smith et al., 2011; Bhatia & Breaux, 2018]. In this paragraph, different definitions are discussed. Solove [2006] found that privacy seems to be about everything, and therefore it appears to be nothing, which indicates why there have been and still are no universal definitions of privacy. Nissenbaum [2012] argues that privacy and data sharing are contextual, which means that it depends on what kind of data is being shared and through what type of device. Hughes [2015] explains that the origin of privacy lies in the subjective desire of individuals to avoid having his/her personal information used to harm the individual. The study concludes that privacy is a claim to control personal information, and it matters because its misuse can cause unjust harm. Solove [2006] argues that not all data collected can be considered as harmful, but certain kinds of collections can be. In a review, Nissenbaum [2012] conceptualizes privacy as contextual integrity, which is a model with the constructs of context-relative informational norms. The critical parameters of informational norms consist of actors (subject, sender, recipient), attributes (type of information), and transmission principles (constraints under which information flows). Furthermore, Dinev et al. [2013] argue that privacy is often referred to as a state in which an individual is found in a given situation at a given moment. This definition is in line with the privacy definition of Pietro & Mancini [2003, p. 78] "the freedom of not having someone or something to interfere in our life without our permission". Smith et al. [2011, p. 995] found that in research the concept of privacy often is referred to as a state, such as "a sought-after goal: an individual's desire to exist in a state of privacy".

Differences in importance of privacy do also occur in the literature, as Solove argues that privacy is "a fundamental right, essential for freedom, democracy, psychological well-being, individuality, and creativity" [Solove, 2008, p. 5]. On the contrary, Moor [1997] argues that privacy is not a "core value" to the fundamental of human evolution, as privacy is not found to be a value in all human cultures. Moors' core values are as stated: life happiness,

freedom, knowledge, ability, resources, and security.

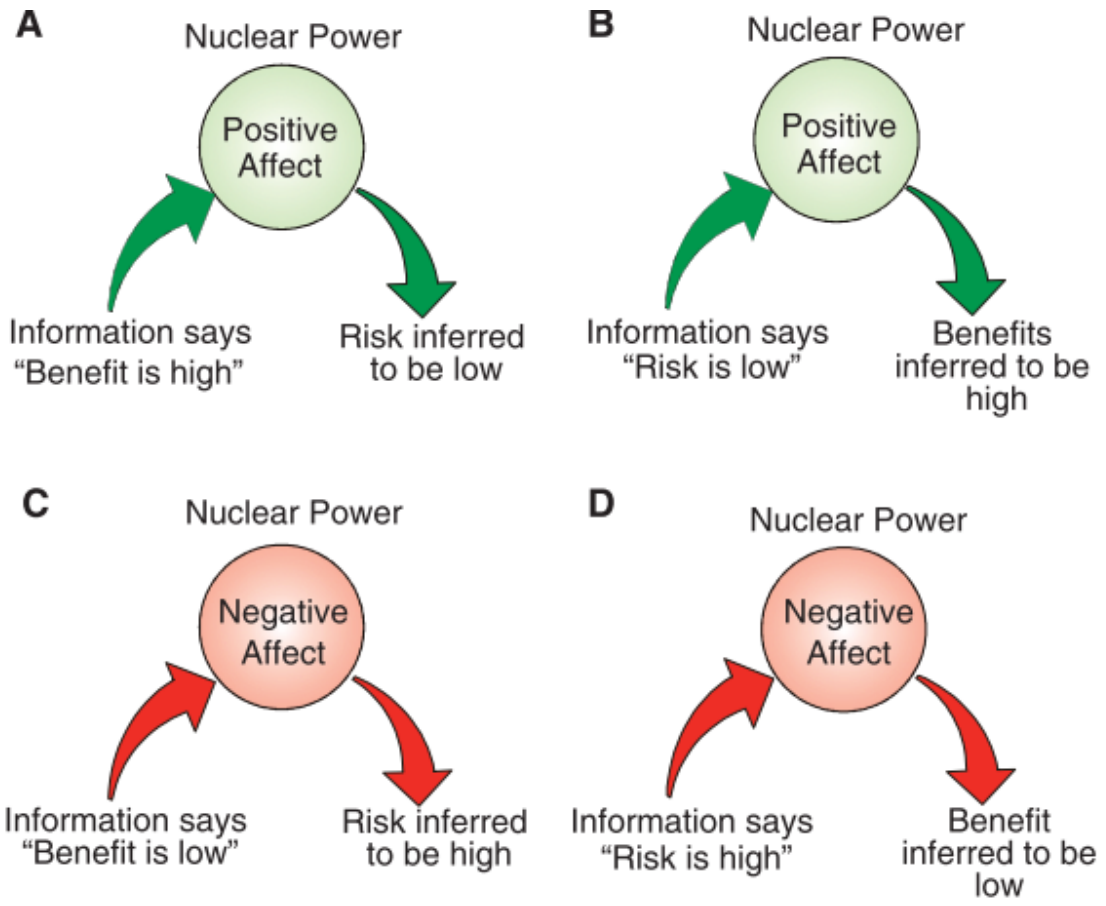
Burgoon [1982] defines privacy through four different dimensions: Physical privacy, social privacy, informational privacy, and psychological privacy. Physical privacy represents personal freedom form surveillance and means total isolation from others in the extreme case. Social privacy represents the ability to regulate the distance in social relationships, either by withdrawing from social intercourse or by the establishment of more closeness. Informational privacy refers to as the individuals´ control over the process and the transfer of personal information. An example of information privacy is the way modern societies collect, store, and process personal information, such as medical data or customer data. Psychological privacy represents the ability to control emotional or cognitive inputs and outputs. Outputs describe the freedom to whom, when, and what personal feelings and thoughts are disclosed. Outputs represent the protection from the emotional interference of others through persuasion. Smith et al. [2011] distinguish two dimensions of privacy, one being information privacy, which in the literature often is referred to as privacy, whereas physical privacy is the other dimension. The difference between these two is that information privacy is the concern of access to identifiable personal information and physical privacy is the concern of physical access to an individual or the individual's private space.

2.2 Privacy and Risk Perception

People do not continuously think about risks of every activity or action they do in everyday life. Instead, people rely on automatic and fast intuitive risk judgments, commonly known as risk perception, and stated as subjective judgments. They are often shaped by the news media or past experiences [Slovic, 1987]; this mode of thinking is known as experiential thinking or affective attitude [Slovic & Peters, 2006]. The concept of risk in the modern world is acted and perceived in two fundamental ways. On one hand, danger can be perceived in an intuitive and instinctual manner and is called risk as feelings. The guidance of feelings and emotions is also referred to as affect heuristic by Slovic & Peters [2006].

On the other hand, the perception of danger can be guided by reasoning and scientific contemplation and is often based on the measured risk-cost-benefit evaluation. This concept is referred to as risk as analysis [Slovic & Peters, 2006]. One reason for the distinguishment is the tendency of experts to assess risks by analysis and statistics rather than relying on emotions. In contrast, non-experts, referred to as laymen in the literature, are more prone to rely on their emotions, when facing danger [Haque, 2000; Digmayer & Jakobs, 2016]. This distinguishment becomes more extensive, the more complex the technologies become, creating a more considerable gap between perceived and actual risk [Fischhof, 1995]. Affect heuristic shares the same fundamental principle as the description of Russell [2003] about core affect. Core affect basis is an emotion from a dimensional perspective in an object-less domain, explaining the relationship between mood and emotions, from Oatley & Johnson-laird [1987]. These object-less dimensions with supporting evidence are as follows; Pleasure

or valence (goodness or badness) and energy or arousal (high or low) [Russell, 2003]. The framework of Russell [2003] describes the core affect, and the affective quality (perception of the core affects' qualities of stimuli) as primitive. A core affect comes within a person as a non-reflective feeling (the person feels angry). In contrast, the affective quality is a perceived stimulus (seeing the sign makes make the person angry) and can cause a change in the core affect. "An object is the person, condition, thing or event at which a mental state is directed" [Russell, 2003, p. 147]. Two strong emotions that often play a role in the risk of feelings are fear and anger. These two appear to have the opposite effects in risk estimates; fear appears to amplify risk estimates, whereas anger reduces them [Lerner et al., 2003]. Lerner et al. [2003] propose that fear arises from estimations of uncertainty and situational control and for fear, the opposite occurs, from certainty and individual control. Slovic & Peters [2006] mentions that people mostly are in a calmer state of judgement and directed by weaker feelings. Slovic & Peters [2006] modified a model based on affect heuristic explaining information to stimuli regarding high benefit, or low risk has a positive affect of the stimuli, which could reduce risk perception of the stimuli or perceive the stimuli as more beneficial. The opposite affect could happen when the information of stimuli is reported to be beneficially low or having a high risk. This results in the perceived risk to be higher or perceived to be less beneficial, see Figure 2.1.



Figur 2.1: Model based on the affect heuristic. The model gives an insight when the information of a given stimulus is being presented has high benefits, therefore, positive affect and in return could lower the risk perception, as in example A. Furthermore at example B, when the information is given that stimuli it has a low risk and therefore a positive affect, the perception of this stimuli could be perceived as beneficially high. The opposite effect happens when the information of the affects to the stimuli is being presented as negative, by having low benefit, example C and high-Risk example D. Modified model by Slovic & Peters [2006], original model by Finucane et al. [2000]

Affect heuristics are influenced by risk characteristics, which describes the activities that have an impact on risk perception other than knowledge are as listed: familiarity, personal control, voluntary, dreaded, and benefits [Slovic et al., 1981]. In the following short examples will be presented of how the risk characteristics can be interrupted as: When an action is familiar, then the action tends to be perceived as less risky. When a person has personal control, then driving a car seems to be perceived as less risky, than flying an airplane as a passenger. When voluntary settling near a nuclear power plant tends to be perceived as less risky for a chemical spill, than a nuclear power plant being involuntary build near your house. When dreaded about a low probability terrorist attack being perceived as risky than falling over a non-dreaded household item - delayed effect. When gaining benefits from an activity results that the activity is being perceived as less risky because of acceptance in the riskiness from the desire of gaining pleasure [Slovic et al., 1981; Slovic, 1987]. Other researchers support the notion of exchanging sensitive information, in this case, location data for benefits or convenience [Zickuhur, 2012]. Digmayer & Jakobs [2016] made a literature analysis about risk studies and found that less than 5% were about

privacy risk, and the majority of risk studies 80% were about technical risks.

Stoycheff et al. [2019] found perceptions of government surveillance suppress individuals' behavior of activities online, through chilling effect and deterrence. The chilling effect explains people's behavioral change of inhibition of there actual actions, this is to reduce repercussions against them. An example in surveillance would be that a person uses other phrases of words to avoid being linked to misunderstandings a form of self-censorship. Suppressed activities include illegal activities and political activities. They found no significant change in online privacy-protective behavior. Privacy protective online behaviors in the study consist of the basic means to secure one's online identity, such as deleting browser history, cookies, and changing passwords. Stoycheff et al. [2019] argues that it could be because the actions only include commonly practiced actions among the general population, so the general population understood the given questionnaire. Another study suggests an opposite effect occurs when surveillance is leaked to the public, which made a spike in users take action in the use of more sophisticated privacy-protective measures, such as using Tor that gives access to become anonymous on the internet [Bodó, 2015]. One of many conceptual tools to explain mass surveillance is explained by the panopticon metaphor. A user might know that they can be tracked after a leak that has been exposed, but the user might not know when exactly they are being tracked. As the panopticon, the prisoners do not know if the inspection in the middle is tracking them at the moment, but they do see the inspection tower in the middle [Foucault, 1995]. McMullan [2015] argues that unlike the panopticon the prisoners know that they likely are being watched. People on the internet might not be aware, because of the invisible factor of surveillance. It was not until the leak from Snowden that the operation of NSA mass surveillance became known for the public, and awareness of this topic arouse into people's perception of their own internet footprint.

Another study used a measuring tool to measure privacy risk perception found even with a high privacy risk perception, adaptation of privacy protection strategies does not seem to be affected except for the use of pseudonyms, cookies cunchers, anonymous email, safe email, and providing false personal data. Which argues that it still leaves to privacy paradox unresolved [Oomen & Leenes, 2008].

The phenomena of privacy paradox describe how users are willing to partake the action of losing their privacy while having concerns about their privacy being violated [Berendt et al., 2005; Williams et al., 2016]. This describes that the users are concerned about their privacy, yet still opt-in to use the service when confronted by the privacy policies when confronted before using the service. Williams et al. [2016] found through surveying the literature five factors that support why privacy paradox occurs. The five factors are education and experience, usability and design, privacy risk salience, social norms, policies, and configurations. Williams et al. [2016] stats that the factors are not mutually exclusive. A literature review of the privacy paradox by Kokolakis [2017] concludes there is still a need for a theoretical model for privacy paradox. Solove [2020] argues that the privacy paradox is a myth and should not be an indicator of how much people value their privacy. Instead, it implies behavior involving risk, where many factors may influence people's decisions. The

paradox does not exist, as it is created on faulty logic and unwarranted generalizations. The conflict between behavior and attitude occurs because behavior is evaluated of the decision making about risk in a very specific context. Whereas attitude is measured in a general context of privacy.

A systematic review by Gerber et al. [2018] analyzed 181 articles of privacy attitude and behavior, found which factors influence risk perception for privacy with a moderate degree: The user's trust of data collector to protect the data collected, Risk-benefit in the gain of personalization compared to data disclosure and the perceived relevance of the collected information.

Wilson et al. [2019] explains by reviewing articles about measures of risk perception, that risk perception is multidimensional and should be included and measured as such. Dimensions for this are affective, severity of consequences, and the probability of the risks occurrence. The first two factors are experimental components of risk and correlates to risk perception. Whereas the probability of the risk occurrence correlates to behavioural intentions or actions of risk. Thus when only measuring attitudinal perceptive of risk, the experiential dimensions are sufficient as measurement dimensions.

2.2.1 Privacy concern and Privacy attitude

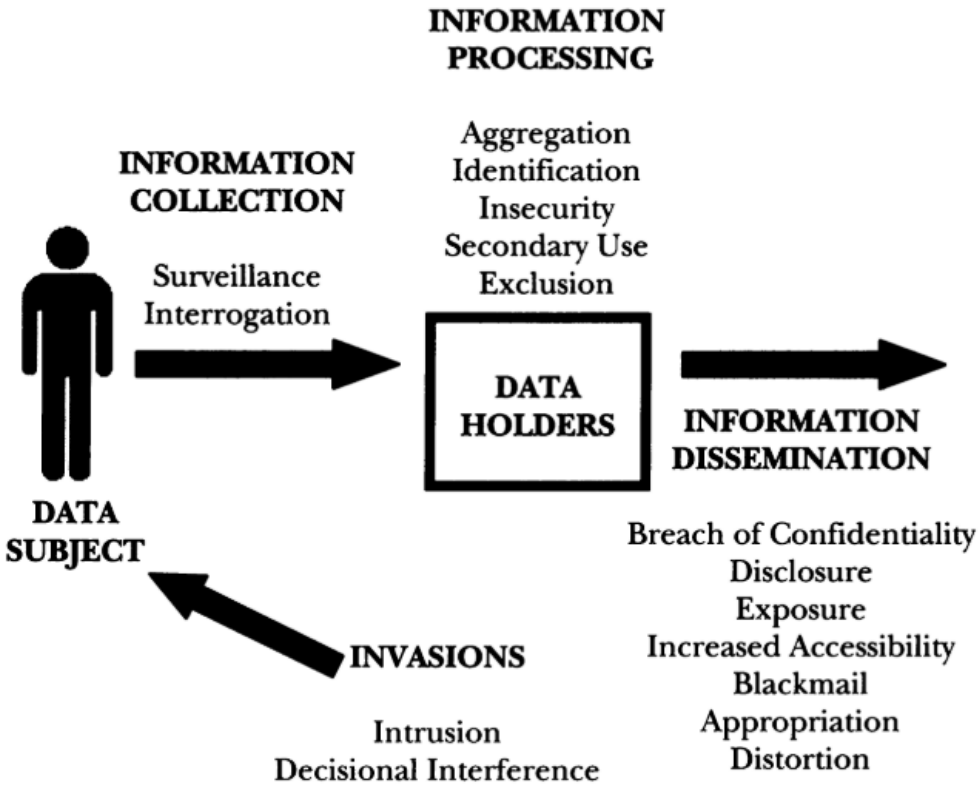
Privacy concern is described as "the desire to keep personal information out of the hands of others" [Buchanan et al., 2007,p. 158]. It captures the negative valence attitude when privacy is being violated by others in an online environment [Dienlin & Trepte, 2015]. Examples of these negative attitudes could be questions about online identity theft, misuse of personal data, or fraud in the communication process. Attitudes on the other hand generally capture both positive and negative attitudes. The most acknowledged view of attitude is "an attitude represents an evaluative integration of cognitions and affects experienced in relation to an object ... Attitudes are the evaluative judgments that integrate and summarize these cognitive/affective reactions" [Crano & Prislin, 2006, p. 347]. The polarity of these two concepts is therefore not the same. As a privacy attitude can be considered positive or negative as in a reflection of two opposing dimensions, bipolar scales can be made to measure attitudinal variables. Whereas privacy concerns only have a negative dimension and varying on the same dimension, the unipolar scale has to be considered [Dienlin & Trepte, 2015]. As privacy concern carries a negative connotation in the concept of information privacy, it may not be adequate to measure privacy perception but acts as a proxy to privacy perception.

Privacy concern can be viewed as dependent or independent variable in the scope of concepts. Smith et al. [2011] found that repeated measures studies primarily have been made with privacy concern as the independent variable. I.e. variables that are course of the concept of privacy concern and have a strong relationship are, how privacy concern affects behavior, trust and regulations. When privacy concern is regarded as the dependent variable, i.e. what courses this concern, examples such as privacy experience, privacy

awareness, personality differences, demographic difference, and culture/climate can be drawn out of the literature, these models have a tenuous relationship to privacy concern, and more repeated studies are needed to confirm these [Smith et al., 2011]. In the relationship between privacy concern and privacy attitude, Dienlin & Trepte [2015] finds privacy concern as the antecedent to privacy attitude. The next section will be looking at the harmful effects that may happen for the individual when privacy is being misused.

2.3 Privacy Harms

Different kinds of privacy harms can directly harm an individual and in this section a closer look at classifications of what these harms can be. Solove [2006] has created a taxonomy model of privacy which explains four basic groups of harmful activities that affect privacy: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion, see figure Figure 2.2. The model begins with the individual affected by the privacy scenario whose life is most directly affected. This is called the data subject. The next step in the model is information collection, this consists of two subgroups, Surveillance, and Interrogation. Solove explains surveillance is when the individuals' activities are being watched, listened to, or recorded. These can describe the sensors in everyday devices, explicitly IoT-devices in today's statue quo of devices. Another form of information collection is via interrogation, which consists of actively probing for information from the user, an example is by asking the user questions. The next group is after the information has been retrieved from the user of the previously mentioned information collection subgroups, and is called information processing. This group consists of five subgroups: aggregation, identification, insecurity, secondary Use, exclusion. These subgroups describe the following processes happening in the information processing group: those that collect the data (called data holders), the processing, storing, combining, manipulating, searching, and using it. The information collectors can be individuals or organizations such as businesses and the government. After the data holders have processed the information, the next group is information dissemination. This group consists of sending the gathered and processed information further from the individual to another entity or release the information. The last group is invasions, this group has a direct impact on the data subject, this group does necessarily not involve information. Arrows in the model describe how the data is either moving further apart from the data subject or closer and directing the data subject.



Figur 2.2: Taxonomy model of privacy which explains the four basic groups of harmful activities that affect privacy: (1) Information collection, (2) information processing, (3) Information dissemination, and (4) invasion. The model begins from the data subject. The first 3 groups (1,2,3) distances the information from the data subject, whereas the last group (4) interferes with the data subject, original model by [Solove, 2006].

Solove [2006]'s taxonomy has been criticized by Bartow [2006] due to a lack of horror examples because it fails to identify ways that negatively impact lives beyond feelings of unease. Solove counter argues with the same argument when people fail to see all of the augmentations and viewpoints of the counter arguments for nothing-to-hide-argument and he expresses that people often have a visceral mindset when this topic is debated. Solove explains few horror cases of people that have obtained sensitive information from companies and used to do bodily harm to a specific individual and if this was the standard case to acknowledge problems, then very few privacy problems will be acknowledged [Solove, 2007]. Furthermore, Solove [2007] explains a counterargument of nothing-to-hide-argument which focuses on why privacy is important other than people using the information to do bodily harm. The explanation is one element of information is nothing that can be used against or in favor of an individual, yet over time an accumulation of elements can be merged together, with the intent to map or something similar to the individual. The need for more research in this area of privacy can be seen in a literature review from Kokolakis [2017] of privacy attitudes and privacy behavior. It concludes with the need for more research in the field of privacy for the diversity of privacy harms, which is an important variable that should be investigated.

2.4 Privacy, security, policies, data protection

Data privacy regulations such as General Data Protection Regulation (GDPR) is to regulate and establish rules of how producers of services have to handle sensitive data and privacy policies, which came into force in May 2018 for European countries [Parliament & Council, 2016]. Privacy policies explain what data is being collected while using a service. Many of the studies in this literature review take aspect in privacy policies as the studied privacy protection. Security's context of privacy can be viewed as a protection of theft from third party organizations, such as hackers [Kalakota & Whinston, 1997]. The organizations can breach the security of the services and access the data and course harm, the harms of theses can be seen at Section 2.3.

2.5 Privacy and Privacy Risk in Human-Computer Interaction

Murphy [1996] finds benefits in a legal regime that protects privacy, by utilizing privacy as a reputation factor and utilizing the increase of willingness of people to engage in activities that they would not have otherwise due to anonymity. This makes anonymity an important factor to make people more willing to engage in activities. Lin et al. [2012] found evidence that properly informing participants of the usage of data collection, the participants felt less uneasy about using an application that uses the phone's GPS data constantly than when it is just requesting to use the GPS data, without any explanation. This type of information collection can be called passive data collection [Onnela & Rauch, 2016] or surveillance when viewed as harm as explained in Section 2.3. This type of data is generated without any participation or action from the user, examples of this generation can be GPS data, or when having a conversation the audio data could be recorded, by phone or similar device with a microphone near the conversation. This surveillance phenomenon can be viewed as a privacy or security breach, if the company owning the service goes against its own privacy policies (privacy breach), or when a service is hacked by a third-party organization (security breach). Furthermore, could this be considered as a risk, because the user does not have knowledge if the passively obtained information is used to improve or as harm. A wide-scale real-life example of this phenomenon is the Chinese social credit score system. China's social credit score can be a concern for the individual because the tracking of the individual's actions and interactions, which can be used to construct representational profiles, map patterns, and behaviors of an individual. These action decisions can affect the social credit score, which either improves or harms the individual by a punishment-reward system [Wong & Dobson, 2019], which supports the notion of nothing-to-hide argument as seen in Section 2.1. Wong & Dobson [2019] furthermore argues stricter data use policies need to be in place or else a similar loss of freedom may occur the western society. Internet-of-thing-devices may be used to sample behavioral data as they can be considered as live trackers and this can especially be a privacy concern when the devices are a connection to the internet and spreading data to the companies and beyond if the data is sold to others.

2.6 Internet-of-Thing-devices

Smart objects are one of many connotations that describes the new flow of devices that are interconnected with each other over the world wide net using internet protocol (IP) [Vasseur & Dunkels, 2000]. Other connotations of this technology are The Internet-of-Things (IoT), web of objects, web of things, and cooperating objects. In this study the connotation IoT-devices will be used to describe this technology, and to emphasize the focus will be on the physical product connected to the internet. The compound of IoT-devices would be having equipped a certain type of sensor or actuator, a microprocessor, a communication device, and a power source. The sensor reads the physical world, the microprocessor transforms the data from the sensor, the communication devices forward the data to the world, for example, another IoT-device or receive input from another IoT-devices. The power source provides the electricity, so the IoT-device can work. Any smart product contains to main behavioral properties, and they are as listed: Interaction with the physical world and communication. The properties of interaction with the physical world are by sensing it with sensors and controlling with actuators. From measuring the air humidity to more complex measures such as air pollution. In this study the terminology "smart" followed by an object that is going to be considered as an IoT-device such as a smart speaker.

2.7 Surveillance and IoT-devices

Studies have shown that some IoT-devices such as Google home's smart speaker do not record or send data unless it has been activated by vocalizing the activation word "OK Google" [Perez et al., 2018]. In other words, Google home's smart speaker does have active data collection and do not have passive data collection. Perez et al. [2018] continues stating the companies do not have to disclose directly to the consumer when their IoT-devices policies have been edited. It is up to the consumer to be up to date, by actively checking on the official website of the product. A study on the covering of webcams by Machuletz et al. [2018] found that privacy concerns do not influence user's decision of utilizing protective webcam covering. They argue that user would rather decide on benefits and disadvantages of inconvenience when using the protective cover, than deciding by evaluating the risk, hence privacy paradox. This is supported in a study by Barth et al. [2019], which controlled for technical knowledge, privacy awareness, and financial means despite the respondents' claims to have a concern about privacy, they still remained unwilling to invest either money or time in privacy protective measures. The authors' questions, if privacy as a concept is conceptualized or not. Solove [2020] supports this notion that even if people can self-management their privacy-protective measures, they perceive it as an infinite task for each service used. Solove [2020] continues stating that people have a threshold for when they have pushed enough buttons when self-management their privacy that they give up and resign the control of their privacy. Self-management privacy might be good in theory as people can control their privacy, in practice it does not work as the tasks

become daunting. Privacy fatigue may have an impact on self-management privacy [Oh et al., 2018]. Machuletz et al. [2018] suggests designing products to protect privacy that are highly usable, intuitive, and easy to understand. Furthermore, they found that perceived social norms influence users' decisions to protect their privacy.

2.7.1 Project Alias - Parasite

An example of physical protective privacy measures is an attachment for Google home called Alias; a teachable parasite Karmann & Knudsen [2018]. It can be attached on top of the microphones of either Google home first edition of smart speaker or Amazon Alexas first edition of smart speaker. By attaching it on top of the devices, it actively blocks the microphones by low static noise and thereby, eliminating any kind of information collected from the devices, hence surveillance. The philosophy of this attachment is to give the user more control over customization and privacy by making it a middle-man device. Alias has its own pair of microphones and speakers. Alias listens and can, if wanted, translate or manipulate a user's command to something else. An example would be a voice command given to Alias: "Hey Alias", this is then translated to "OK Google"from Alias, and therefore activating the smart speaker without using the command "OK Google". This is one of the highlights with more customization, as the user cannot change the google activation command from "OK Google"as-well-as Alexa's "Hey Alexa".

In a sense it moves the problem area from producers of the smart speakers to Alias in terms of surveillance. Despite the fact that the Alias project is open source, bigger cooperations such as Google smart speaker are not.

2.8 Privacy and security perception assessment studies

Through an interdisciplinary review of privacy research, Smith et al. [2011] argues that is near impossible to asses privacy itself and privacy assessment depends on privacy-related measures. These related measures are often referred to as beliefs, attitudes, and perceptions. The information system discipline is making a move to have a central construct called privacy concern. This construct is commonly adopted proxy to privacy, yet Dinev et al. [2013] beliefs that privacy concern is not identical to general privacy. Reasons for this distinction are there is no rigorous definition of privacy, the lack of literature that describes privacy concern in the light of general privacy and that privacy concern carries a negative connotation to general privacy and information privacy, as this may be inadequate if general privacy should be regarded as valuable. Their definition of general privacy is adapted from Furthermore, as to general privacy, the problem has been that scholars had struggles of formulating what exactly general privacy is - behavior, state, function, or feeling.

A construct in social science is the assessment of personal characteristics, they can either be direct such as height (cm) or weight (kg), etc or indirectly such as the level of a state as in

depression, happiness, or other states. Indirect constructs can not be measured directly and therefore use numbers of indicators or items which are measurable and they are considered underlying to the construct [Cronbach & Meehl, 1955]. Privacy perception has been found through studies that it is not one dimensional [Dienlin & Trepte, 2015; Burgoon, 1982; Dinev et al., 2013]. Furthermore Dayarathna [2013] states it is very difficult to build a methodology to quantify information privacy or the measures used to protect information privacy. Yet explains by including risk assessments will then be able to assess information privacy. Risk assessments are a combination of identifying the risks, an assessment for the severity of the risks, and strategies to manage the identified risks.

One study by Dinev et al. [2013] tested two major factors for privacy perception without the physical privacy factor: perceived information control and perceived risk, the constructs could explain 52% of the variance for perceived privacy. Thus more factors would be needed to explain more of the variance. They explained another construct voluntariness could have the possibilities to fit into the interplay of control, privacy, and risk, as they argue that other websites where personal information is not given freely can be viewed differently. Chang et al. [2015] Uses the created constructs from Dinev et al. [2013] to develop a boundary management model. They found that Privacy control affects perceived privacy and risk influences perceived privacy. Furthermore, they highlighted that two proxies to perceived privacy were privacy concern and trust.

Other studies [Dienlin & Trepte, 2015; Trepte & Reinecke, 2011] used Burgoon [1982] privacy dimensions described in Section 2.1 to explain privacy perception and behavior in an online environment. Yet they did not use the physical dimension, as it serves no purpose in the cyberspace domain.

Buchanan et al. [2007] made a 16-item measurement scale to measure privacy concern online. Items that do not correlate with this study are not included and therefore taking out. IoT-devices can be considered as semi-online services, as they act with the internet yet are in the physical world and therefore not applicable to use privacy concern measurement tools. Furthermore Smith et al. [1996] constructed a 15-item instrument to measure concern about information privacy in the context to privacy concern including 4 constructs: collection, errors, secondary use, and unauthorized access to information. This instrument has been then further used to construct and validate a joined latent construct called CFIP (Corncern for information privacy) Stewart & Segars [2002] which they found to have a high validation and reliability. They also found computer anxiety to correlate with CFIP, and the higher the anxiety is the higher CFIP is. Many of the above-mentioned studies have their own meaningful constructs of privacy perception, attitude, or belief. A thorough search of the relevant literature yielded that Xu et al. [2012] creates the physical privacy factor in relation to surveillance, called perception surveillance. Furthermore, many of the articles in this chapter capture the general attitude instead of a specific attitude. An example of a general attitude can be seen in Smith et al. [1996] which measures individuals' concern about organizational practices. Every question is general, one of the observable variables from the collection dimension asks: "It usually bothers me when companies ask me for personal information". If a user has a high score in CFIP that suggests that: (1)

immoderate amount of data is collected, (2) a large amount of the data is inaccurate, (3) corporations use personal information for undisclosed purposes, and (4) corporations fail to protect access to personal information.

Attitudinal scales can change meaning after time because structures in life changes as do attitudes toward objects and perceptions Smith et al. [1996]. Therefore, it might not be functional to use attitudinal privacy instruments that were constructed before IoT-devices became more normalized in the current time. This indirectly include that the existing measurement tools might not be applicable in the current time.

2.8.1 Cognitive state measurement

As mentioned earlier, the literature is struggling to define privacy, and Dinev et al. [2013] argues that much of the literature defines privacy implicitly as a state, which has made a survey through the literature. This study adapts that privacy can be considered as a state from Dinev et al. [2013]. Thus making a testable definition of privacy as perceived (state of) privacy. This can be translated into by Dinev et al. [2013,p. 299] "perceived privacy is an individual's self-assessed state in which external agents have limited access to information about him or her". Cognitive states can be measured from three different perspectives, performance measures, psychophysiological measures and subjective measures [Kramer, 1990].

Performance measures build on covert performance such as error rate and task completion time. These measures are objective and provide a real-time assessment of the user's cognitive state [Karwowski, 2006]. Psychophysiological measures like performance measures are an objective measure and capture the physiological bodily change to physiological manipulation these are mostly involuntary. Subjective measures unlike the other two are based on overt measures. These are dependent on the user's perception of tasks [Kramer, 1990]. Subjective responses may be directly influenced by the respondents' characteristics such as answering style, interpretation of questionnaire, social disability, and limits of memory [Kivikangas et al., 2010]. It is not possible to assess subjective measures in real-time and usually taken after a condition or activity.

2.8.2 Questionnaire usefulness

The usefulness of a questionnaire to measure the general privacy perception of specific objects such as an IoT-device. May be when designing products that have to yield a high privacy perception or to test to see if the privacy perception is sufficient. This assessment tool may then be used in conjunction with other perception scales such as sensory descriptors to figure out what exactly scores high in privacy perception. Furthermore, studies has found, as described in the review that usability is not good enough for the privacy solution, and therefore explores that the risk of losing privacy is valued less, if the usability is insufficient in relation to cost-benefit relationship. Therefore, in terms of

using the questionnaire in human-computer interaction may yield new knowledge on how to ensure a better privacy without the cost of usability, as both have to be measured.

3 | Aim of the study

Projects like Alias subsection 2.7.1 provide a privacy-protective measure. However, the effectiveness of this product regarding perceived privacy has not jet been assessed. It is questionable if the user perceives more privacy when having Alias connected to the smart speaker, as privacy issues may be transferred to Alias. Outcome variables, such as a change in behavior, will not be taken into consideration in this study, except for attitudinal state change as a test of the experimental design [Smith et al., 2011]. In the literature, no specific assessment instrument was found to measure the privacy perception of IoT-devices with respect to protective measures. Therefore, the main focus of this study is to design a scale to assess the general privacy perception toward an object and then use it in an experimental context.

The aim of this study leads to the following research question:

> *How can privacy perception with respect to IoT-devices protective measures be assessed?*

Subsequently, research questions that are addressed in this study are:

- What constructs for privacy perception do already exists in the literature and how can they be accommodated for IoT-devices?
- How can these constructs be used for the assessment of privacy perception?
- How can these constructs be tested to test for validity and reliability?
- Does the scale work in an experimental setup?

Dinev et al. [2013] creates a nomological network that explains general privacy perception, but in the context of web browsing in Web 2.0. This nomological network does not include the physical factor to privacy perception as derived from Burgoon [1982]. This connection is explored in the following chapter to include this factor with the help from other studies. Firstly, a PPS is designed by mainly using the constructs as described in Dinev et al. [2013]. However, the constructs are modified to this study's needs. The PPS is then validated and tested, by comparing the assessment tool scores between two scenarios and assessed by a reliability test.

4 | Construction of privacy protection perception assessment instrument

In this chapter, the used method to design the PPS for IoT-devices and focus on privacy-protective measures is explained.

4.1 Scale development

Smith et al. [1996] created a process model for the development of instruments and the validation of these. The process model contains three main stages. In the first stage the domain and dimensionality of the construct are specified, items are generated, the content validity is assessed. The process model is based on literature review, experience surveys, focus groups and expert judges.

The second stage administrates the instrument and then explores it with two statistically strong correlating instruments; Exploratory factor analysis (EFA) and Confirmatory factor analysis (CFA) [Diana, 2006]. EFA explores the underlying factor structures for observed variables without prior and prepositions. CFA uses knowledge and empirical research to postulates the relationship pattern as a prior and then testes the relationship between observed variables and their underlying latent constructs. A resourceful assumption for these two methods is that the sample size should at least count 100 respondents for analysis done by EFA and for testing by CFA the sample size should be 5-20 times the variables. In the last step validity and reliability is assessed by CFA and Pearson correlations. Moreover,the generalizability is assessed. These steps were executed in an assessment period of three years [Smith et al., 1996]. Due to this amount of resources required, a less rigorous methodology will be used in order to develop the instrument. The scale development is based on literature study and previous constructs and results from the literature review. The items will be edited and deleted in order to accommodate for experiment purpose.

4.2 Construct modification

Different dimensions of privacy perception exist. Smith et al. [2011] Distinguishes between two dimensions for privacy after reviewing the literature, the first being information privacy and the second being physical privacy. Dinev et al. [2013] uses information privacy in another context, and therefore not entirely the same context-wise, as explained before in Section 2.8. The constructs that will be used to create the scale are: perceived information collection and perceived risk, as stated in Dinev et al. [2013]. The physical variable, perceived surveillance, will be adapted from Xu et al. [2012]. Perceived surveillance can be considered as a physical construct according to Burgoon [1982]. The observable variables will be adjusted to reflect physical IoT-devices and the passive usage i.e. by being in close proximity to the IoT-device, yet without using it actively.

The risk perception observable measures described byDinev et al. [2013] were not used in this study. Wilson et al. [2019] suggested using affect and severity to measure risk perception. Affect questions were developed with inspiration from the general risk perception construct questions of Dinev et al. [2013]. They were modified in order to measure the physical privacy and passive surveillance of the device. Furthermore, they were then transformed to measure the affective dimensions of risk perception, see Digital Appendix Section F.1. The constructs for perceived severity were modified from a validated study of Xue & Liang [2010]. The items were adjusted to a single item as stated in Gerber et al. [2019] and adjusted to fit this questionnaire´s design. The specific constructs have been modified to be used in an experimental setting. This procedure can be seen in Digital Appendix Section F.1.

4.3 Constructs explanations

As described before,privacy perception is multidimensional. These dimensions will be explained in this section by the use of the constructs of privacy perception.

4.3.1 Perceived privacy risk

According to Wilson et al. [2019] perceived privacy risk can be measured by adding an affect component and a severity component together, which indicates the consequences of a risk. This is then multiplied by the probability of the risk with exposure and vulnerability. In this study, affect and severity will be used for a measure of perceived privacy risk. The affect construct typically measures negative emotions, such as worries, fears, etc. Whereas severity measures the severity or magnitude of the consequence experienced.

4.3.2 Perceived privacy control

Tactics of information control refers to tactics of managing how consumers control the amount and accuracy of their shared information. Dinev et al. [2013], have modified them to perceived privacy control, and describes it as "mechanisms for maintaining the desired state of privacy"[Dinev et al., 2013, p. 300] by controlling the amount of shared information. The three tactics are: anonymity, secrecy and confidentiality. Anonymity is describe as concealment of the identity of the person itself. Secrecy is described as concealment of information with the intention of concealing the information shared. Confidentiality refers to keep the already stored information by a device from unauthorised people, as perception of the information must be protected [Dinev et al., 2013].

4.3.3 Perceived surveillance

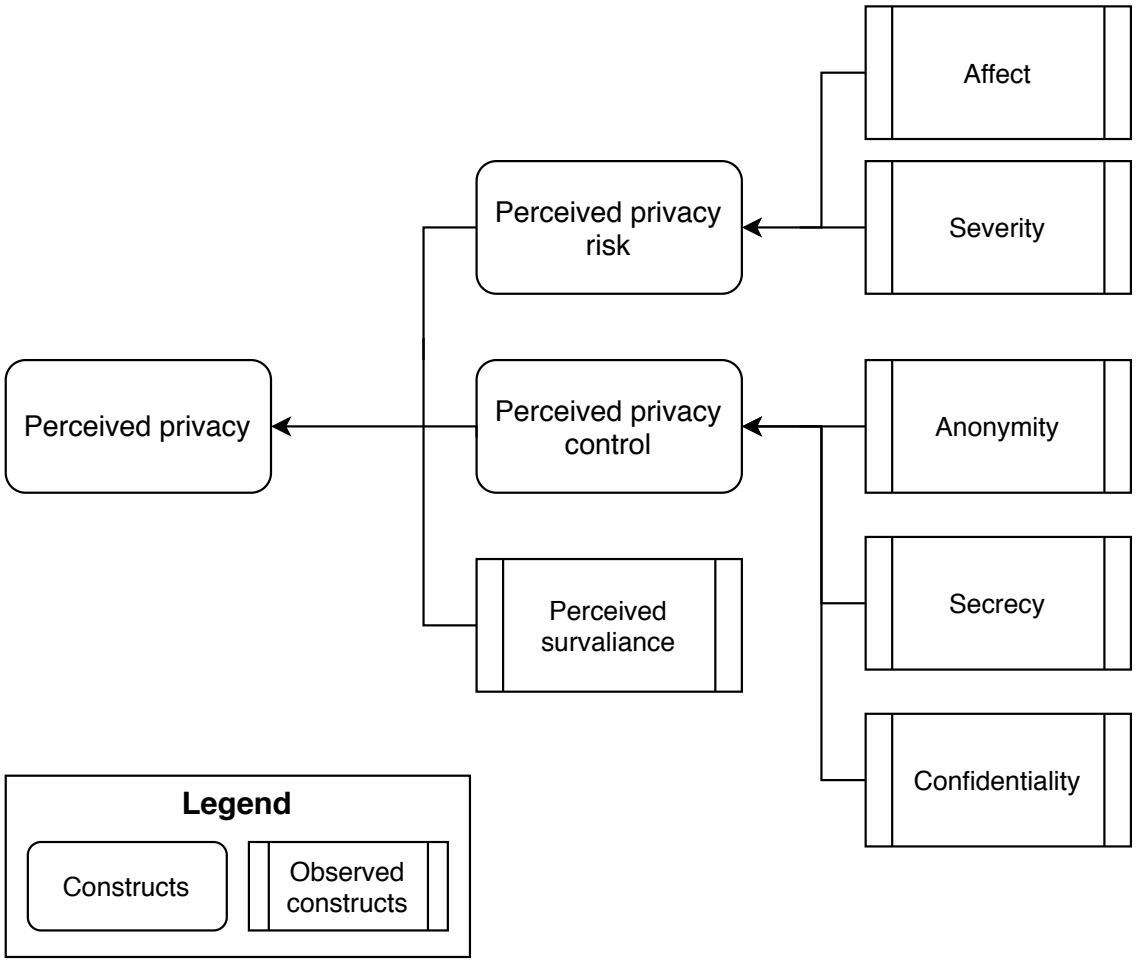
Perceived surveillance is the practice of data collection, and does not distinguish between legal or illegal data collection [Xu et al., 2012].

4.3.4 Perceived privacy

The state of privacy, captured by all the underlying constructs: perceived privacy risk, perceived privacy control and perceived surveillance. See Section 2.1 for further detail.

4.3.5 Proposed instrument to measure privacy protection

A visual representation of how each of the underlying construct are connected with perceived privacy i seen in figure 4.1. Construct being explored are perceived surveillance, anonymity, secrecy, confidentiality and affect. Figure 4.1.



Figur 4.1: Proposed privacy protection assessment instrument with its constructs and observable measures connected with each other to the main construct, privacy perception.

4.4 The process of adding, deleting and modification of construct items

The transformation of the construct items was made in 7 steps and can be seen in Digital Appendix Section F.1. The transformation was made to use already existing and validated questions and then transforming them into questions with specific attributes. For example "these web sites" was transformed to "this smart product". Thereafter, the questions were modified to specific questions instead of general questions, as the privacy perception is measured when using the device. The word "concerned" from the surveillance construct of Xu et al. [2012] had been changed to "believe" as this is displays the same method of wording as used in Dinev et al. [2013]. Questions have been deleted in order to reduce the number of items to 13 items, as before the questionnaire had 35 items. All items from Dinev et al. [2013] that captured the proposed underlying factors of privacy risk perception were removed, and instead general question of privacy risk perception were formed. The questions have been transformed to include the passive component of being near a product and to capture the risk of a physical device. Furthermore, the questions

have been transformed to get an affective meaning, such as "I would feel uncomfortable...", as recommended by Wilson et al. [2019]. Then the items have been transformed from being possibilities, as there is always a possibility of something collecting data into factual questions. The final items for each construct can be seen at Table 4.1. The ID of the construct as shown in the table, are their abbreviation. Their real names are as follows: Risk refers to affect construct. ANYT refers to anonymity construct. SCRT refers to secrecy construct. CFDT refers to confidentiality. SUR refers to surveillance. Sev refers to Severity. The true order refers to how it is shown in the questionnaire, where one is the first item that is shown, and two is the next, the order have been randomized, using a randomizer, see Digital Appendix Section F.1. Severity construct items can be seen in Table 4.2.

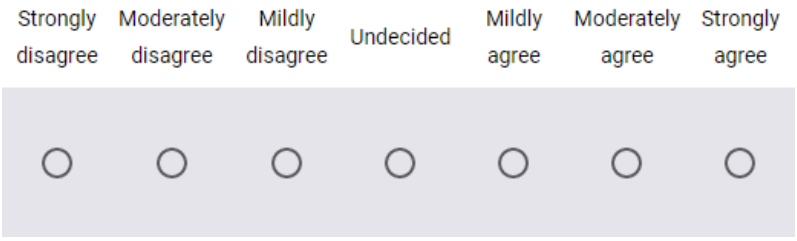
True order	**ID**	**Measurement item**
9	Risk1	I feel uncomfortable revealing personal information about me close to the smart speaker.
11	Risk2	There will be a high potential for privacy loss revealing personal information close to the smart speaker.
1	Risk3	I am afraid that the smart speaker will use personal information, revealed in close proximity to it, in an inappropriate way.
3	Risk4	I am concerned that revealing personal information close to the smart speaker will involve many unexpected problems.
12	ANYT1	I believe I can hide my true identity using this smart speaker.
6	ANYT2	The information is kept anonymous on this smart speaker.
4	SCRT1	I believe I can conceal some information from this smart speaker when I want to.
2	SCRT2	I believe I can refuse to give my personal information to this smart speaker when I think it is too personal.
8	CFDT1	I believe my personal information provided to this smart speaker remains confidential.
5	CFDT2	I believe my personal information is accessible only to those authorized to have access.
13	SUR1	I believe that the smart speaker will obtain information while having it in close proximity when doing other activities.
10	SUR2	I believe that this smart speaker is collecting too much information about me.
7	SUR3	I believe that my conversation is monitored by this smart speaker.

Tabel 4.1: This table shows the final PPS. It displays the true order, which has been randomized when used in an experiment. The ID of the construct as shown: Risk refers to affect construct. ANYT refers to anonymity construct. SCRT refers to secrecy construct. CFDT refers to confidentiality. SUR refers to surveillance. Sev refers to Severity. All the measurement items - observable values. And all the measurement items - observable values.

True order	**ID**	**Measurement item**
14	Sev1	Assuming that the topic was recorded by the smart speaker, this would be...
15	Sev2	Assuming that the topic was only recorded by the smart speaker if it were in use, this would be...

Tabel 4.2: This table shows the final PPS for the severity construct of risk perception. It contains the true order, which has been randomized when used in the experiment.

A 7-point likert scale is used for all the first 13 items for the PPS; ranging from "strongly disagree"to "strongly agree", with a middle point of "undecided", see figure Figure 4.2. The reason for using a 7-point likert scale, is because of the familiarity of the format. The PPS may be used in a complex scenario based experimental setup, thus making the scale more familiar to reduce the complexity for the participant.



Figur 4.2: 7-point likert scale used for the first 13 items of PPS.

4.5 Interpretation of scale values

Two out of five constructs in the instrument have to be reversed coded before interpretation. These two items are; perceived privacy risk and perceived surveillance. Going forward with the interpretation of the instrument after reveres coding, a low score indicates a state of having low privacy and a high score indicates a state of having high privacy.

The method to summarize the score is described in [Bangor et al., 2008], the specific method explanation can be seen in Digital Appendix Section F.2. As this questionnaire aims to find the general privacy perception from a given situation, which aligns with how the system usability scale tries to find the general usability of a usage. A limitation for using this method of summarizing is that usability is one dimensional, and it may not be an effective method of summarizing, as the general privacy perception questionnaire does have more than one dimension.

5 | Validation of instrument

In this chapter the PPS will be tested in an experimental setup, using online respondents.

5.1 Methodology

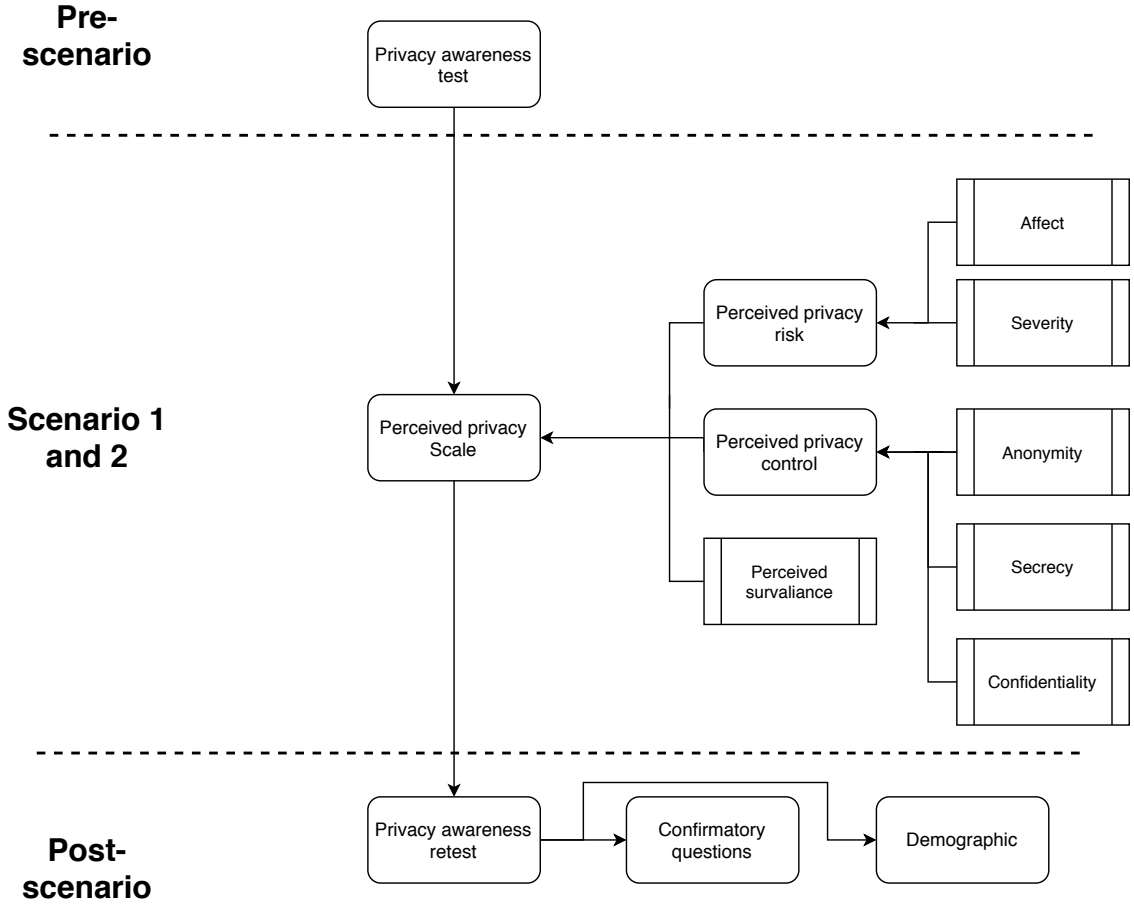
The method of testing the PPS was done with an A/B-testing method with within-subject design. This had been conducted by the use of a survey, which contains two different scenarios. Whereas the scenarios are the independent variables. These include a control variable which consists of the default smart speaker. The experimental condition, covers for the surveillance opportunity, and therefore the assumption is that this creates a high perceived privacy in terms of passive surveillance. The objective with this experiment is to test if the instrument is measuring perceived privacy in terms of protective measures.

Another way to measure peoples judgement and attitudes is to use the factorial survey experiment method (FSE) or vignette experiment for surveys [Liebe et al., 2020]. Yet in this method, two factors are used, one control the other experimental. The focus is to test whether the scale works for the indented purpose of measure. The same concepts of having scenarios are used, yet in a simple method. The validation will be conducted using a survey structure, and therefore acts as a survey study. Furthermore, factor extraction is carried out for the first scenario, in this study referred to as condition, as the second condition may be effected by a carry-over effect. Two different analyses are performed, one to check for reliability of the items and constructs them self, and the next is to check if the PPS works in the desired experimental setup for its use.

5.2 Survey study development

The survey is constructed to test the designed PPS and assess if it measures for privacy perception by using two extreme bipolar scenarios, where the control condition has low privacy and the experimental condition has high privacy. It all depends on the user, therefore it cannot be stated that either of the scenarios are either high in privacy or low in privacy. To some people both scenarios can either be true or false in scenarios. Therefore, it is assumed people that are aware of privacy threats might find this distinguishment

acceptable or not enough. The structure and procedure of the survey can be seen in Figure 5.1. The survey structure explains what and when the participant are going to see each part of the survey. In the following sections, each of the steps are going to be explained in more detail. The survey can be seen in Appendix C.



Figur 5.1: A diagram to illustrate the flow of the survey. In the pre-scenario, the privacy awareness scale is used. After each scenario, the privacy perception scale is used. Post-scenario the retest of privacy awareness is measured, demographics, and confirmatory values.

In this survey, the number of items will be described as follows, three questions from privacy awareness and 15 from PPS. Times two, because they are asked again after the second scenario. Two confirmatory questions. Six general questions. In total 44 questions are asked throughout the survey.

5.2.1 Scenarios

The different scenarios have been created to demonstrate two extremes in privacy perception. The scenarios are based around having the sensors for a smart product covered or uncovered. In this case a Google home smart speaker has been chosen, albeit the chosen smart speaker is not stated in the survey. It has only been stated that it is a smart speaker, in order to avoid trust factors for the specific brand of smart speaker. As referenced to

in subsection 2.7.1, measures have been created to create more privacy for the user. The whole concept of Alias has not been implemented in order to reduce the complexity of the scenario. Therefore, in this case an understandable approach has been chosen where a Alias lookalike was created in this study to shields for the microphone sensors, and can then be uncovered by activating a button, see Appendix B.

The scenarios are chosen to be hypothetical in order to avoid personal and ethical consequences. This means that the participant do not have to base their sensitive information on their own information, instead they just have to assume the scenario. The scenarios are abstract according to Gerber et al. [2019] as participants do not know the consequences if their information is spread to unknown or known sources. Examples of specific use cases can bee seen in Gerber et al. [2019].

The contextual of the scenarios are the same in order not to introduce unnecessary confounding variables. The only contextual difference except for the Alias lookalike, is the difference that the participant is talking to a friend in the first scenario and a family member in the second scenario. The scenario is based upon giving sensitive information to a reliable person. And in both cases the smart speaker is in proximity of this hypothetical conversation, the participant have to imagine. The Alias lookalike is used as this item captures a sense of device. Another item would have had the same ability to be used in the scenario, as the purpose was just to illustrate that it covers the microphone holes. By using this lookalike, the respondent have some sense that they can interact with the product, instead of removing an item on top of the Google home speaker.

5.2.2 Classification of the public

According to Westin's studies of privacy awareness in a index made by Kumaraguru & Cranor [2005], classification of the public can be grouped into three different levels of general privacy awareness groups. Fundamentalist - High privacy concern, Pragmatist - medium privacy concern and unconcerned - low privacy concern. The privacy fundamentalist are the most protective of their privacy. These respondents feel that organizations should not collect personal information for the organizational own needs and think that people should be proactive in refusing giving in of personal information. The privacy pragmatist based their willingness to share personal information according to pros and cons of sharing the information. They evaluate the protections that are in place and also based on their trust to the company or organization. The privacy unconcerned are the least protective of their privacy. They feel that providing information to organization far outweigh the potential harm of sharing the information. Lastly they do not favor expansion of more privacy protective regulations. See questionnaire and method for classification in Appendix A. It is chosen to have the privacy awareness scale as the first questions, as they are general in nature, and specific questions can influence general questions found. These general question are also used as a retest to see if the survey influence the participants perception of general privacy.

5.2.3 Control variables

The affect heuristic, could have an effect on how people would perceive the risk. Therefore, no negative or positive information about the stimuli are made, because it could affect the perception of being less or more risky. This may not be the option as Dayarathna [2013] stated that without knowing the risk and understanding the consequences of it, a privacy assessment can not be captured. Therefore, in the questionnaire, it is described what the device does and what sensors are active in the designated scenarios. As the survey was made in spring 2020, in the middle of a world pandemic, people may experience another form of everyday life and have an unknown feeling that could translate into being less risky or more in the given context of sharing privacy or medical information. Therefore, this could be a confounding factor. Being more risky in giving personal and medical information to track the spreading of the COVID-19, as the benefits might be higher for society. The respondants could also be more concerned to privacy, as authorities have a reason to do mass surveillance as seen in China [Lu, 2020]. Gerber et al. [2019] used the work experience in the field of IT security, as a student, researcher or practitioner to determine if people are experts or lay people respect to privacy. This study will use the same method to classify the difference. If the respondent answers more than one year of experience, they are then considered as experts, otherwise as lay people. If respondent have some kind of experience, they are then considered to be an expert in this survey. The country of the respondent have been asked, as the survey has been distributed into the world wide web. Culture differences may affect the results on perceived privacy.

5.3 Pilot testing the questionnaire

The questionnaire were reviewed by two people. One pointed out fewer questions per page would be more ideal to ensure that the item values were seen (Disagree to agree). And the other could not understand the difference between the last two likert confirmatory questions. One of the confirmatory questions were edited to have a negative meaning. Other than that, the question were well understood, as-well as the scenarios and how to rate them. After further analysis, the severity items have been extracted out of the PPS as they do not serve a meaning-full relationship, if they were to be summarized as a total score. They can be used as confounding factors instead.

5.4 Distribution of survey

This thesis is written in the middle of an ongoing pandemic in the world and the local area. It is then not possible for ethical reasons to distribute in the local communities, as the distributor and respondents will have an increase possibility to get infected by the COVID-19 virus. A telephonic distribution is not optimal due to conceptualization of the scenario will not be adequate when the questionnaire is given. The respondent have to

visually see the different conditions in order to fully grasp the state of privacy between the conditions. The chosen method of distribution of the survey in these circumstances is an online distribution method. The distribution will be administrated into different fora so it can capture a homogeneous populations, see Appendix D of the chosen fora and their text in danish and English. The survey was created in SurveyXact from Ramboll [2020]. The instrument was in english and the recruitment was spread out as much as possible to get most participant. The survey was open for two weeks from the 26Th of April 2020 and closed 10Th of May. A responds rate of 15% (46 respondents), 7% (21 respondents) of somewhat finished and total distribution to 297 people. A distribution can be counted multiple times, as the survey was distributed anonymously, which means every click on the link to the survey will count as a new distribution. The data analysis will exclusively be reported on the respondents that fully completed the survey. All the respondents were informed that their data will be kept anonymous, and that they could withdraw at any point.

5.4.1 Participants

A total of 46 respondents (19 male, 25 female and 2 others) completed the survey. The age of respondents ranged from 20 to 45 years (M = 27, SD= 5.7). See the overall characteristics of the respondents in Appendix Table E.1.

5.5 Statistical analysis

The statistical method is split into two sections. The first section is about how sufficiently the items of the scales are intercorrelated. The next section is about how the two different conditions perform on the questionnaire. The last section will be looking into confounding variables, which may have had an effect on the results of the conditions. The statistical analysis and calculations was done in SPSS, version 26.0.0.0, unless otherwise specified. The data can be found in Digital Appendix Section F.2, called "Raw_data" and "All_Data_reverseCoded".

Testing the individual items betweem one another

The quality of an assessment scale is usually assessed in terms of its content validity, construct validity and reliability [Straub & Gefen, 2004]. Content validity is either backed up by literature review or expert domain evaluation. In this study the content validity is backed up on previous studies based on literature review, and combination of other theories which is then merged together to create a measurement instrument for this study specific use case. Construct validity is usually based on three other validates: convergent validity, discriminant validity and nomological validity. Construct validity can be established if convergent validity, discriminant validity and nomological validity are acceptable. Convergent validity are measures or variables that correlate positively with each

other within the same construct. Discriminant validity distinguishes if two constructs are similar, which they should not be, as they will then measure the same concept. Nomological validity is the theoretical approach of predicting ways scales correlates with each other distinct but related constructs.

The data will not be tested by a CFA because of the low sample size N = 46, an EFA will be used. Before testing for factors and reliability, a factor extraction method was computed on the data. This is to ensure that the correct amount of factors are extracted form the data. Normally the eigenvalue-greater-than-one rule from Kaiser is used, while this extraction may be common in statistical program, it may not be the most sufficient way of determining the amount of factors. In order to get a reliable eigenvalue cutoff value, a parallel analysis has been considered, as it takes the number of items and number of respondents into account[Thompson & Daniel, 1996]. The parallel analysis found that one factor should be extracted from the data and all latent constructs from privacy control have been reversed coded, see Appendix Section E.2. A PCA was run on the 13 items from the questionnaire for condition 1 of 46 respondents. Inspection of the correlation matrix showed that all variables had at least one correlation coefficient greater than 0.3. Item ANYT1 had one correlation with a coefficient of 0.327 to sur1. The overall KMO was 0.876 which is a measure for adequacy of the variables, and value above 0.8 shows the sampling is adequate [Kaiser, 1974].

Cronbach's α is used to examine the reliability of the scales and their internal consistency between items in order to determine, how well they are measuring the same underlying dimension. In other words, how well the items are grouped together [Yu, 2001]. Cronbach's α is used for each of the scales, as it cannot determine dimensionality. As there is only one factor, the Cronbach's α is used for all the items.

Condition scores

The scored likert data is ordinal, as the distances between each score do not have a definite meaning. However, in this data analysis, the likert data is considered as continuous. Parametric tests are known for having a higher statistical power than non-parametric tests and, therefore, parametric test were considered for further analyses even if the data is ordinal from likert scale Carifio & Perla [2008]. One of the assumptions for using ordinal data as continuous, is that the likert scale has at least five categories in order [Sullivan & Artino, 2013]. As the likert scale in this study had seven categories in order, this assumption was fulfilled. Because the likert data was positively skewed and the Shapiro-Wilk test was significant, a normality of the pairwise differences was not asserted as seen in Appendix Section E.4. Therefore, the statistical analysis of the likert data were addressed with non-parametric test within the realm of pairwise testing between the conditions. The pairwise comparison was performed with Wilcoxon signed-rank test. One assumption for Wilcoxon signed-ranked test is the data have to be close to a symmetric distribution. Therefore, the difference scores were visually inspected by a histogram. As shown in the Appendix E, Figure E.10. Moreover, the histogram was approximately symmetrically distributed. The effect size of non-parametric tests was calculated by dividing Z by the square root of the

sample size [Tomczak & Tomczak, 2014]. The confounding variables were tested for gender, age and privacy awareness. All the tests can be seen in Section E.6. The test are only used on condition 1, as the carry-over effect may have a high deflection on condition 2. A visual inspection of the pre -and post categorizations of the privacy awareness classification was carried out to examine if people have been affected by taking the questionnaire.

5.6 Results - Factor

As mentioned before, a parallel analysis found that only one factor is adequate to be computed according to the eigenvalue. Each of the components loading's can be seen in Table 5.1. It shows that anyt1 has a low loading, whereas item anyt2, scrt1 and scrt2 have a medium loading. The rest have a high loading. As there is only one factor, it is possible that privacy perception may not be multidimensional. Furthermore, the components of the PPS will be named privacy perception, as there is only one factor.

Loading	
	Component 1
risk1	.813
risk2	.875
risk3	.790
risk4	.822
anyt1	.269
anyt2	.652
scrt1	.555
scrt2	.474
cfdt1	.846
cfdt2	.771
sur1	.843
sur2	.795
sur3	.852

Tabel 5.1: Loading's for component 1 for each item of condition 1.

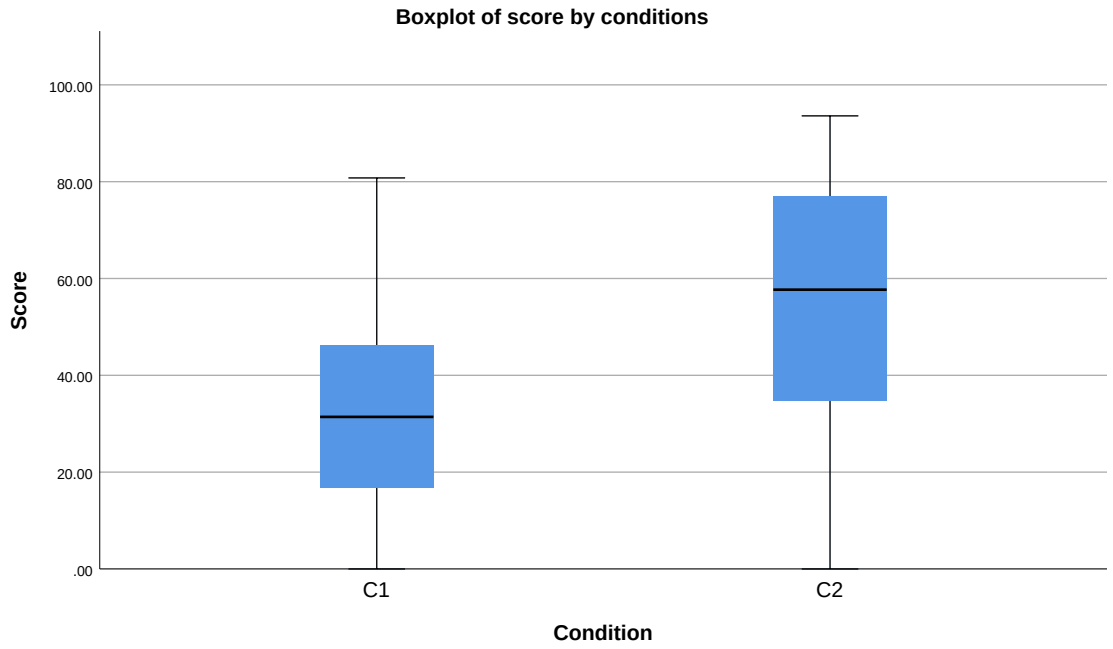
When checking for reliability, Cronbach's α is used. The main construct, consists of 13 items had a high level of internal consistency, as determined by a Cronbach's α of 0.924. When assessing how the items fit within the scale, a item-total correlation was tested, see Table 5.2. A item-total correlation value less than 0.3 indicates that the item it self does not correlate amongst the overall scale values, thus may be dropped [Churchill, 1979]. It can be seen that item anyt1 has a score of .239, thus indicating that it may not measure the same as the rest of the items.

	Item-total correlation
risk1	.753
risk2	.832
risk3	.741
risk4	.768
anyt1	**.239**
anyt2	.589
scrt1	.520
scrt2	.434
cfdt1	.792
cfdt2	.712
sur1	.800
sur2	.731
sur3	.802

Tabel 5.2: Overview of item-total correlation between all items of the questionnaire.

5.7 Results - Conditions

The descriptive data for each of the conditions' items can be seen in Appendix Section E.3. Out of the 46 respondents, 41 had an increased privacy perception in condition 2 compared to condition 1, whereas four respondents had a decreased privacy perception and one saw no improvement, see Figure E.10. A Wilcoxon signed-rank test determined that there was a statistically significant increase in the privacy perception score ($Mdn = 15.38$) when respondents perceived condition 2 ($Mdn = 57.69$) compared to condition 1 ($Mdn = 31.41$), $Z = 5.43$, $p < 0.001$, $r = 0.80$. A visual representation between the two conditions' medians can be seen in Figure 5.2.



Figur 5.2: Boxplot of mean scores for condition 1 (C1) and condition 2 (C2).

5.8 Confounding factors

The confounding variables were compared with condition 1's summarized scored of privacy, as carry-over effect may have effected the answers for condition 2. All the calculations for the confounding variables can be seen in Appendix Section E.6. A visual inspection of a scatter-plot for condition one and age was made and did not reveal a monotonic or linear relationship. Therefore, a correlation could not be calculated by the Spearman´s correlation. It was checked if gender is a confounding factor by conducted Mann-Withney U test of condition 1 and gender. The test revealed no significant difference between males (Mdn = 29.49) and females (Mdn = 32.05) (U = 236.5, Z = -.024, p = .981). To assess if privacy awareness was a confounding factor a one-way ANOVA was carried out. There was found homogeneity of variance, as assessed by Levene's test for equality of variances (p = .354). The test revealed that the privacy score were lowest for fundamentalist (n = 18, M = 21.58, SD = 17.91), whereas pragmatist (n = 25, M = 39.64, SD = 20.29) and unconcerned (n = 3, M = 41.02, SD = 9.25), had a relatively same mean between each other and higher mean than fundamentalist. The one-way ANOVA revealed that there was a statistically significant difference in privacy awareness classification groups and privacy scores, $F(2, 43) = 5.044$, $p < 0.011$, 2 = .190. In conclusion a significant difference between fundamentalist and pragmatist was found, where fundamentalist have a lower score than pragmatist for condition 1.

5.8.1 Test-retest of privacy awareness

Descriptive data of privacy awareness and classification for the participant pre- and post-scenarios can be seen in Table 5.3. The calculation can be seen in digital appendix F.2. It can be seen that it had an effect on some respondents to being more aware of privacy due to the questionnaire. From condition 1 to condition 2, the number of pragmatist increased from 18 to 24 respondents. Whereas the number of unconcerned has decreased from three to zero respondents.

	Fundamentalists	**Unconcerned**	**Pragmatists**
Pre	39.1%(18)	6.5%(3)	54.3%(25)
Post	52.2%(24)	0%(0)	47.8%(22)

Tabel 5.3: Classification of the respondents pre- and post-scenarios. The number of participants are shown in parenthesis.

6 | Discussion

The aim of the study was to design a PPS to measure the user´s privacy perception of IoT product regarding to protective measures. The PPS was assessed for its reliability in an experimental scenario. In this section, the results of this experiment are discussed.

In general, the results of the experiment suggest that the designed PPS can be used in order to assess the users´s privacy perception of IoT devices regarding to protective measures.

Factor analysis

As described in the results, the EFA suggest one factor. This could be caused by the respondents not having a direct interaction with the device, thus they did not perceive control, as there was no direct control to perceive. Furthermore, it does indicate that some items have a high loading, primarily from the affect construct and surveillance construct. Item ANYT1 scored a low cronbach's alpha value and a low item-total correlation. This indicates that this item do not measure the same as the other items. The items is as follows: "I believe I can hide my true identity using this smart speaker". It can be argued that the word "using", may not have been adequately used for the specific experimental set-up, as no interactions were possible in the hypothetical scenarios. As the ANYT1 was the only question that did not fit into the questionnaire it is proposed to either change the question into a passive question or to use the PPS in an active scenario. As the PPS ultimately was designed to be used in an active scenario, where participants could interact with the device, it is believed that this could change the perception of the participant toward the question. It is hypothesized that the ANYT1 would fit into the questionnaire, when used in an active scenario.

The PPS was designed to have five underlying constructs, but only one factor was found. This means that the questions did not underlie multiple constructs, but just one general construct, privacy perception. In conclusion, the scoring of the PPS can be calculated by adding all questions together, rather then using the five factors as ultimately proposed.

Condition - Scores

As expected the two conditions of perceived privacy are significantly different. It indicates that even when the respondents had to responds to a hypothetical scenarios, the difference would still occur between the condition. It was expected that the scores of condition 2 are higher than the assessed scores, as it operates in an extreme scenario. The hypothesis has been confirmed by the experimental study. The method of summarizing the scores worked, as only one factor was discovered for the scenario, thus making a summarizing of all the scores to be an adaptable method. If EFA revealed more than one factor, the method of scoring would have been different, as scores for each of the factors, instead of a summarizing of the items scores.

Confounding factors

Confounding factors such as age and gender did not have an influence on privacy perception. The privacy awareness scale showed a difference, where fundamentalist had a lower score than pragmatist, in other words, a lowered state of privacy. This means that the scale might be more useful in order to see an effect if people with a fundamentalist mindset are asked. This means that the more privacy aware a person is, the lower the score of for PPS when testing without a protective measure on an IoT-device.

In conclusion, the hypothesis of a difference between condition 1 and two was fulfilled, thus, suggesting that the PPS measures the privacy perception of IoT device users. Furthermore, the factor analysis suggests that only one factor is present and therefor, summarizing all scores is possible. Lastly, the privacy awareness of the participants reveled to be a confounding factor, suggesting a combination of the privacy awareness questionnaire and the PPS to be optimal.

6.1 Limitations

This research focuses on privacy perception, attitude and beliefs. Thus, it does not value the outcome variables that can changes state or behaviour. Due to resource limitations CFA could not be conducted and instead a EFA was conducted. Therefore, this study is missing a strong statistical analysis of the underlying factor structures and validation of the factor structures of the observed variables [Diana, 2006]. A rigorous validation process and reliability have to be tested in order to verify the usage of the instrument. The experimental design included hypothetical scenarios, instead a real life scenarios may have been better to reflect the actual perception. Validating the PPS using an experimental set-up might not be the best solution when testing for validity. It is suggested that the PPS is tested in only one scenario, instead in an a experimental set-up with two conditions.

The following variables severity, confirmatory questions, expert vs. laymen relationship,

were tested but not further analysed. As there could be a difference in the privacy perception of experts and laymen it is proposed to analyse this relation in further studies.

7 | Conclusion

The present study aimed to design a PPS for IoT devices. The experimental study to assess for the reliability of the designed PPS revealed that the PPS can be used in order to assess the user´s privacy perception of IoT devices regarding to protective measures. In the factor analysis, only a factor was extracted by conducting a PCA and parallel analysis. The cronbach α value of the factor was found to be .924. The item ANYT1 has a low loading and low item-total correlation of .239, which indicates that this item does not measure the same as the other items. Therefore, this particular question needs to be reconsidered as discussed. It was found to be a significant difference between control condition and experimental condition using the PPS, with $r = .80$. Whereas the control condition were perceived having a state of less privacy than for the experimental condition.

7.1 Future work

The items that are not intercorrelated with the rest of the items need to be corrected. Furthermore, validating the instrument by performing a CFA with a substantially larger sample size, would be beneficial to confirm the validity of the instrument. Another EFA can be explored with a larger sample size in order to confirm if the questions of the PPS underlie only a single factor, as shown in this study.

Moreover, the relationship between privacy perception and user experience would be an interesting study, especially when IoT-devices become standard devices in households and smart cities slowly emerges into the societies.

Bibliography

Bangor et al., jul 2008. Aaron Bangor, Philip T. Kortum & James T. Miller. *An Empirical Evaluation of the System Usability Scale*. International Journal of Human-Computer Interaction, 24(6), 574–594, 2008. ISSN 1044-7318. doi: 10.1080/10447310802205776. URL `http://www.tandfonline.com/doi/abs/10.1080/10447310802205776`.

Barth et al., 2019. Susanne Barth, Menno D.T. de Jong, Marianne Junger, Pieter H. Hartel & Janina C. Roppelt. *Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources*. Telematics and Informatics, 41, 55–69, 2019. ISSN 07365853. doi: 10.1016/j.tele.2019.03.003. URL `https://doi.org/10.1016/j.tele.2019.03.003`.

Bartow, 2006. Ann Bartow. *A Feeling of Unease About Privacy Law*. University of Pennsylvania Law Review, 155(52), 52 – 62, 2006.

Berendt et al., 2005. Bettina Berendt, Oliver Günther & Sarah Spiekermann. *Privacy in e-commerce : Stated preferences vs. actual behavior*. Communications of the ACM, 48(4), 101–106, 2005. ISSN 00010782. doi: 10.1145/1053291.1053295.

Bhatia & Breaux, dec 2018. Jaspreet Bhatia & Travis D. Breaux. *Empirical Measurement of Perceived Privacy Risk*. ACM Transactions on Computer-Human Interaction, 25(6), 1–47, 2018. ISSN 1073-0516. doi: 10.1145/3267808. URL `https://dl.acm.org/doi/10.1145/3267808`.

Bodó, 2015. Balázs Bodó. *Piracy versus privacy: An analysis of values encoded in the pirate browser*. International Journal of Communication, 9(1), 818–838, 2015. ISSN 19328036.

Buchanan et al., 2007. Tom Buchanan, Carina Paine, Adam N. Joinson & Ulf-Dietrich Reips. *Development of measures of online privacy concern and protection for use on the Internet*. Journal of the American Society for Information Science and Technology, 58(2), 157–165, 2007. ISSN 15322882. doi: 10.1002/asi.20459. URL `http://doi.wiley.com/10.1002/asi.20459`.

Burgoon, 1982. Judee K. Burgoon. *Privacy and Communication*. Annals of the International Communication Association, 6(1), 206–249, 1982. doi:

10.1080/23808985.1982.11678499. URL https://doi.org/10.1080/23808985.1982.11678499.

Carifio & Perla, **dec 2008**. James Carifio & Rocco Perla. *Resolving the 50-year debate around using and misusing Likert scales*. Medical Education, 42(12), 1150–1152, 2008. ISSN 03080110. doi: 10.1111/j.1365-2923.2008.03172.x. URL http://doi.wiley.com/10.1111/j.1365-2923.2008.03172.x.

Chang et al., **2015**. Younghoon Chang, Siew Fan Wong & Hwansoo Lee. *Understanding perceived privacy: A privacy boundary management model*. Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings, (July), 2015.

Churchill, **feb 1979**. Gilbert A. Churchill. *A Paradigm for Developing Better Measures of Marketing Constructs*. Journal of Marketing Research, 16(1), 64, 1979. ISSN 00222437. doi: 10.2307/3150876. URL https://www.jstor.org/stable/3150876?origin=crossref.

Crano & Prislin, **2006**. William D. Crano & Radmila Prislin. *Attitudes and Persuasion*. Annual Review of Psychology, 57(1), 345–374, 2006. ISSN 0066-4308. doi: 10.1146/annurev.psych.57.102904.190034. URL www.annualreviews.org.

Cronbach & Meehl, **1955**. Lee J. Cronbach & Paul E. Meehl. *Construct validity in psychological tests*. Psychological Bulletin, 52(4), 281–302, 1955. ISSN 00332909. doi: 10.1037/h0040957.

Dayarathna, **2013**. Rasika Dayarathna. *Discovering Constructs and Dimensions for Information Privacy Metrics*. PhD thesis, pages 71, 2013. URL http://www.diva-portal.org/smash/get/diva2:617312/FULLTEXT02.pdf.

Diana, **2006**. D. Suhr Diana. Exploratory or Confirmatory Factor Analysis? In *SAS Users Group International Conference*, pages 17, 2006.

Dienlin & Trepte, **2015**. Tobias Dienlin & Sabine Trepte. *Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors*. European Journal of Social Psychology, 45(3), 285–297, 2015. ISSN 10990992. doi: 10.1002/ejsp.2049.

Digmayer & Jakobs, **oct 2016**. Claas Digmayer & Eva-Maria Jakobs. Risk perception of complex technology innovations: Perspectives of experts and laymen. In *2016 IEEE International Professional Communication Conference (IPCC)*, volume 2016-Novem, pp. 1–9. IEEE, oct 2016. ISBN 978-1-5090-1761-4. doi: 10.1109/IPCC.2016.7740510. URL http://ieeexplore.ieee.org/document/7740510/.

Dinev et al., **may 2013**. Tamara Dinev, Heng Xu, Jeff H. Smith & Paul Hart. *Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts*. European Journal of Information Systems, 22(3), 295–316, 2013. ISSN 0960-085X. doi: 10.1057/ejis.2012.23. URL https://www.tandfonline.com/doi/full/10.1057/ejis.2012.23.

Finucane et al., jan 2000. Melissa L. Finucane, Ali Alhakami, Paul Slovic & Stephen M. Johnson. *The affect heuristic in judgments of risks and benefits*. Journal of Behavioral Decision Making, 13(1), 1–17, 2000. ISSN 0894-3257. doi: 10.1002/(SICI)1099-0771(200001/03)13:1<1::AID-BDM333>3.0.CO;2-S.

Fischhof, 1995. Baruch Fischhof. *Risk Perception and Communication Unplugged: Twenty Years of Process*. Proceedings of the American Control Conference, 15(2), 137–145, 1995. ISSN 07431619. doi: 10.1109/acc.2013.6580909.

Foucault, 1995. Michel Foucault. *Discipline and Punish: The Birth of the Prison*, pp. 195–228. Vintage Books, 1995. ISBN 0679752552.

Gerber et al., 2018. Nina Gerber, Paul Gerber & Melanie Volkamer. *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior*. Computers and Security, 77, 226–261, 2018. ISSN 01674048. doi: 10.1016/j.cose.2018.04.002. URL `www.sciencedirect.com`.

Gerber et al., jul 2019. Nina Gerber, Benjamin Reinheimer & Melanie Volkamer. *Investigating People's Privacy Risk Perception*. Proceedings on Privacy Enhancing Technologies, 2019(3), 267–288, 2019. ISSN 2299-0984. doi: 10.2478/popets-2019-0047. URL `https://content.sciendo.com/view/journals/popets/2019/3/article-p267.xml`.

Gonzaga, 2016. School of Business Gonzaga. *Parallel Analysis*, 2016. URL `https://analytics.gonzaga.edu/parallelengine/`.

Haque, 2000. C. E. Haque. *Risk assessment, emergency preparedness and response to hazards: The case of the 1997 Red River Valley Flood, Canada*. Natural Hazards, 21 (2-3), 225–245, 2000. ISSN 0921030X. doi: 10.1023/A:1008108208545.

Hughes, 2015. R. L.David Hughes. *Two concepts of privacy*. Computer Law and Security Review, 31(4), 527–537, 2015. ISSN 02673649. doi: 10.1016/j.clsr.2015.05.010. URL `http://dx.doi.org/10.1016/j.clsr.2015.05.010`.

Kaiser, mar 1974. Henry F. Kaiser. *An index of factorial simplicity*. Psychometrika, 39 (1), 31–36, 1974. ISSN 0033-3123. doi: 10.1007/BF02291575. URL `http://link.springer.com/10.1007/BF02291575`.

Kalakota & Whinston, 1997. Ravi Kalakota & Andrew B. Whinston. *Electronic Commerce: A Manager's Guide*, Firewalls and Transaction Security, pp. 123–134. Addison-Wesley Longman Publishing Co., Inc., USA, 1997. ISBN 0201880679.

Karmann & Knudsen, 2018. Bjørn Karmann & Tore Knudsen. *Project Alias*, 2018. URL `https://bjoernkarmann.dk/project_alias`.

Karwowski, 2006. Waldemar Karwowski. *International encyclopedia of ergonomics and human factors*, Mental Workload Measurement, pp. 504–506. New York : Taylor & Francis, 2006. ISBN 978-0415304306.

Kim, **2013**. Hae-Young Kim. *Statistical notes for clinical researchers: assessing normal distribution (2) using skewness and kurtosis.* Restorative Dentistry & Endodontics, 38 (1), 52, 2013. ISSN 2234-7658. doi: 10.5395/rde.2013.38.1.52. URL `https://rde.ac/DOIx.php?id=10.5395/rde.2013.38.1.52`.

Kivikangas et al., **2010**. Matias Kivikangas, Inger Ekman, Guillaume Chanel, Simo Järvelä, Ben Cowley, Mikko Salminen, Pentti Henttonen & Niklas Ravaja. *Review on psychophysiological methods in game research.* Proceedings of DiGRA Nordic 2010: Experiencing Games: Games, Play, and Players, (May 2014), 2010.

Kokolakis, **2017**. Spyros Kokolakis. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon.* Computers and Security, 64, 122–134, 2017. ISSN 01674048. doi: 10.1016/j.cose.2015.07.002. URL `http://dx.doi.org/10.1016/j.cose.2015.07.002`.

Kramer, **1990**. Arthur Kramer. *Physiological metrics of mental workload: A review of recent progress.* Navy Personnel Research and Development Center, pp. 1–55, 1990.

Kumaraguru & Cranor, **2005**. Ponnurangam Kumaraguru & Lorrie Faith Cranor. *Privacy Indexes: A Survey of Westin's Studies*, (Report No. CMU-ISRI-5-138). Institute for Software Research International School of Computer Science Carnegie Mellon University Pittsburgh, PA, 2005. URL `http://www.pandab.org/RptOrderForm.pdf`.

Lerner et al., **mar 2003**. Jennifer S. Lerner, Roxana M. Gonzalez, Deborah A. Small & Baruch Fischhoff. *Effects of Fear and Anger on Perceived Risks of Terrorism.* Psychological Science, 14(2), 144–150, 2003. ISSN 0956-7976. doi: 10.1111/1467-9280.01433. URL `http://journals.sagepub.com/doi/10.1111/1467-9280.01433`.

Liebe et al., **2020**. Ulf Liebe, Ismaïl M. Moumouni, Christine Bigler, Chantal Ingabire & Sabin Bieri. *Using Factorial Survey Experiments to Measure Attitudes, Social Norms, and Fairness Concerns in Developing Countries.* Sociological Methods and Research, 49(1), 161–192, 2020. ISSN 15528294. doi: 10.1177/0049124117729707.

Lin et al., **2012**. Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist & Joy Zhang. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *UbiComp'12 - Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pp. 501–510, New York, New York, USA, 2012. ACM Press. ISBN 9781450312240. doi: 10.1145/2370216.2370290. URL `http://dl.acm.org/citation.cfm?doid=2370216.2370290`.

Lu, **2020**. Donna Lu. *China uses mass surveillance tech to fight spread of coronavirus.* New Scientist, 245(3270), p.7, 2020. ISSN 02624079. doi: doi.org/10.1016/S0262-4079(20)30378-X. URL `http://search.ebscohost.com.zorac.aub.aau.dk/login.aspx?direct=true&db=aph&AN=141823028&site=ehost-live`.

Machuletz et al., **2018**. Dominique Machuletz, Stefan Laube & Rainer Böhme. Webcam Covering as Planned Behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, volume 2018-April, pp. 1–13, New York, New York, USA, 2018. ACM Press. ISBN 9781450356206. doi: 10.1145/3173574.3173754. URL https://doi.org/10.1145/3173574.3173754 http://dl.acm.org/citation.cfm?doid=3173574.3173754.

McMullan, **2015**. Thomas McMullan. *What does the panopticon mean in the age of digital surveillance? The parallel between Jeremy Bentham's panopticon and CCTV may be clear, but what happens when you step into the world of data capture?* The Guardian (London, England), pp. 1–4, 2015. URL https://search.ebscohost.com/login.aspx?direct=true{&}db=edsggo{&}AN=edsgcl.422823707{&}authtype=shib{&}site=eds-live{&}authtype=shib{&}custid=ns215211.

Moor, **1997**. James H. Moor. *Towards a theory of privacy in the information age*. ACM SIGCAS Computers and Society, 27(3), 27–32, 1997. ISSN 00952737. doi: 10.1145/270858.270866.

Murphy, **1996**. Richard S. Murphy. *Property rights in personal information: An economic defense of privacy*. Privacy, 84(7), 43–80, 1996. ISSN 00168092. doi: 10.4324/9781315246024-4.

Nissenbaum, **2012**. Helen Nissenbaum. *A contextual approach to privacy online*. Digital Enlightenment Yearbook 2012, pp. 219–234, 2012. doi: 10.3233/978-1-61499-057-4-219.

Oatley & Johnson-laird, **1987**. Keith Oatley & P. N. Johnson-laird. *Towards a Cognitive Theory of Emotions*. Cognition and Emotion, 1, 29–50, 1987. doi: 10.1080/02699938708408362. URL https://doi.org/10.1080/02699938708408362.

Oh et al., **2018**. Junhyoung Oh, Ukjin Lee & Kyungho Lee. *Privacy fatigue in the internet of things (IoT) environment*. IT CoNvergence PRActice (INPRA), 6(4), 21–34, 2018. URL www.rimala.net.

Onnela & Rauch, **2016**. Jukka Pekka Onnela & Scott L. Rauch. *Harnessing Smartphone-Based Digital Phenotyping to Enhance Behavioral and Mental Health*. Neuropsychopharmacology, 41(7), 1691–1696, 2016. ISSN 1740634X. doi: 10.1038/npp.2016.7. URL www.neuropsychopharmacology.org.

Oomen & Leenes, **2008**. Isabelle Oomen & Ronald Leenes. *Privacy Risk Perceptions and Privacy Protection Strategies*, volume 261, pp. 121–138. Springer US, Boston, MA, 2008. ISBN 9780387779959. doi: 10.1007/978-0-387-77996-6_10. URL http://www.prime-project.eu http://link.springer.com/10.1007/978-0-387-77996-6{_}10.

Parliament & Council, **2016**. European Parliament & Council. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data*

Protection Regulation) (Text with EEA relevance), 2016. URL https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

Perez et al., may 2018. Alfredo J. Perez, Sherali Zeadally & Jonathan Cochran. *A review and an empirical analysis of privacy policy and notices for consumer Internet of things*. Security and Privacy, 1(3), 1–15, 2018. ISSN 24756725. doi: 10.1002/spy2.15. URL http://doi.wiley.com/10.1002/spy2.15.

Pietro & Mancini, 2003. Roberto Di Pietro & Luigi V. Mancini. *Security and privacy issues of handheld and wearable wireless devices*. Communications of the ACM, 46(9), 74–79, 2003. ISSN 00010782. doi: 10.1145/903893.903897.

Ramboll, 2020. Ramboll. *SurveyXact*. Accessed: 01-05-2020, 2020. URL https://www.surveyxact.dk/.

Russell, 2003. James A. Russell. *Core Affect and the Psychological Construction of Emotion*. Psychological Review, 110(1), 145–172, 2003. ISSN 0033295X. doi: 10.1037/0033-295X.110.1.145.

Slovic, 1987. Paul Slovic. *Perception of risk*. Science, 236(4799), 280–285, 1987.

Slovic & Peters, dec 2006. Paul Slovic & Ellen Peters. *Risk Perception and Affect*. Current Directions in Psychological Science, 15(6), 322–325, 2006. ISSN 0963-7214. doi: 10.1111/j.1467-8721.2006.00461.x. URL http://journals.sagepub.com/doi/10.1111/j.1467-8721.2006.00461.x.

Slovic et al., sep 1981. Paul Slovic, Baruch Fischhoff & Lichtenstein Sarah. *Perceived Risk: Psychological Factors and Social Implications [and Discussion]*. Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 376(1764), 17–34, 1981. URL www.jstor.org/stable/2397115.

Smith et al., 1996. H. Jeff Smith, Sandra J. Milberg & Sandra J. Burke. *Information privacy: Measuring individuals' concerns about organizational practices*. MIS Quarterly: Management Information Systems, 20(2), 167–195, 1996. ISSN 02767783. doi: 10.2307/249477.

Smith et al., 2011. H. Jeff Smith, Tamara Dinev & Heng Xu. *Information privacy research: An interdisciplinary review*. MIS Quarterly: Management Information Systems, 35(4), 989–1015, 2011. ISSN 02767783. doi: 10.2307/41409970.

Solove, 2007. Daniel Solove. *"I've Got Nothing to Hide"and Other Misunderstandings of Privacy*. San Diego Law Review, 44(4), 745–772, 2007. ISSN 0036-4037. URL https://scholarship.law.gwu.edu/faculty{_}publications/.

Solove, jan 2006. Daniel J. Solove. *A Taxonomy of Privacy*. University of Pennsylvania Law Review, 154(3), 477–564, 2006. ISSN 00419907. doi: 10.2307/40041279. URL https://www.jstor.org/stable/10.2307/40041279?origin=crossref.

Solove, 2008. Daniel J. Solove. *Understanding Privacy*. GWU Legal Studies Research Paper No. 420, pages 24, 2008. URL https://ssrn.com/abstract=1127888.

Solove, **2020**. Daniel J Solove. *The Myth of the Privacy Paradox*. SSRN Electronic Journal, pages 41, 2020. ISSN 1556-5068. doi: 10.2139/ssrn.3536265. URL `https://scholarship.law.gwu.edu/faculty{_}publications https://www.ssrn.com/abstract=3536265`.

Stewart & Segars, **2002**. Kathy A. Stewart & Albert H. Segars. *An empirical examination of the concern for information privacy instrument*. Information Systems Research, 13(1), 36–49, 2002. ISSN 10477047. doi: 10.1287/isre.13.1.36.97.

Stoycheff et al., **2019**. Elizabeth Stoycheff, Juan Liu, Kai Xu & Kunto Wibowo. *Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects*. New Media and Society, 21(3), 602–619, 2019. ISSN 14617315. doi: 10.1177/1461444818801317. URL `https://doi.org/10.1177/1461444818801317`.

Straub & Gefen, **2004**. Detmar Straub & David Gefen. *Validation Guidelines for IS Positivist Research*. Communications of the Association for Information Systems, 13, 380–427, 2004. ISSN 1529-3181. doi: 10.17705/1cais.01324. URL `https://aisel.aisnet.org/cais/vol13/iss1/24`.

Sullivan & Artino, **dec 2013**. Gail M. Sullivan & Anthony R. Artino. *Analyzing and Interpreting Data From Likert-Type Scales*. Journal of Graduate Medical Education, 5 (4), 541–542, 2013. ISSN 1949-8349. doi: 10.4300/JGME-5-4-18. URL `http://www.jgme.org/doi/abs/10.4300/JGME-5-4-18`.

Thompson & Daniel, **apr 1996**. Bruce Thompson & Larry G. Daniel. *Factor Analytic Evidence for the Construct Validity of Scores: A Historical Overview and Some Guidelines*. Educational and Psychological Measurement, 56(2), 197–208, 1996. ISSN 0013-1644. doi: 10.1177/0013164496056002001. URL `http://journals.sagepub.com/doi/10.1177/0013164496056002001`.

Tomczak & Tomczak, **2014**. Maciej Tomczak & Ewa Tomczak. *The need to report effect size estimates revisited. An overview of some recommended measures of effect size*. Trends in Sport Sciences, 1(21), 19–25, 2014. URL `http://www.wbc.poznan.pl/Content/325867/5{_}Trends{_}Vol21{_}2014{_} no1{_}20.pdf`.

Trepte & Reinecke, **2011**. Sabine Trepte & Leonard Reinecke. *Privacy Online*, The Social Web as a Shelter for Privacy and Authentic Living. In: Trepte S., Reinecke L. (eds), pp. 61–74. Springer, Berlin, Heidelberg, 2011.

Vasseur & Dunkels, **2000**. Jean-Philippe Vasseur & Adam Dunkels. *Interconnecting smart objects with IP : the next Internet*, What Are Smart Objects?, pp. 3–20. Elsevier / Morgan Kaufmann Publishers, Amsterdam, 2000. ISBN 9780123751652.

Williams et al., **2016**. Meredydd Williams, Jason R.C. Nurse & Sadie Creese. *The perfect storm: The privacy paradox and the Internet-of-things*. Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016, pp. 644–652, 2016. doi: 10.1109/ARES.2016.25.

Wilson et al., apr 2019. Robyn S. Wilson, Adam Zwickle & Hugh Walpole. *Developing a Broadly Applicable Measure of Risk Perception*. Risk Analysis, 39(4), 777–791, 2019. ISSN 0272-4332. doi: 10.1111/risa.13207. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.13207.

Wong & Dobson, 2019. Karen Li Xan Wong & Amy Shields Dobson. *We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies*. Global Media and China, 4(2), 220–232, 2019. ISSN 2059-4364. doi: 10.1177/2059436419856090. URL https://doi.org/10.1177/2059436419856090.

Xu et al., 2012. Heng Xu, Sumeet Gupta, Mary Beth Rosson & John M. Carroll. *Measuring mobile users' concerns for information privacy*. International Conference on Information Systems, ICIS 2012, 3(Ftc 2009), 2278–2293, 2012.

Xue & Liang, 2010. Yajiong Xue & Huigang Liang. *Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective**. Journal of the Association for Information Systems, 11(7), 394–413, 2010. URL https://search-proquest-com.argo.library.okstate.edu/docview/734860834/fulltextPDF/789DD193978441EDPQ/1?accountid=4117.

Yu, 2001. Chong Ho Yu. *An introduction to computing and interpreting Cronbach coefficient alpha in SAS*. Proceedings of the 26th SAS User Group International Conference., 2001. URL http://www2.sas.com/proceedings/sugi26/p246-26.pdf.

Zickuhur, 2012. Kathryn Zickuhur. *Three-quarters of smartphone owners use location-based services*. Report of the Pew Internet And American Life Project, pages 27, 2012. URL https://www.pewresearch.org/internet/2012/05/11/three-quarters-of-smartphone-owners-use-location-based-services/.

A | Privacy awareness scales

In the following, the adapted privacy awareness scale is shown. Beneath it is the transformed privacy awareness based on the original scale.

A.0.1 Privacy awareness scale - Original

Westin's Privacy index - see Kumaraguru & Cranor [2005].

Scale 1-4: (1) strongly disagree to (4) strongly agree

1. Consumers have lost all control over how personal information is collected and used by companies.
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

A.0.2 Privacy awareness scale - transformed and used as retest

Scale 1-4: (1) strongly disagree to (4) strongly agree

1. Companies have taken control over how the personal information of consumers is collected and used.
2. The collection of the consumers' information is handled by most businesses in a proper and confidential way.
3. Today consumer privacy is sufficiently protected by existing laws and organizational practices.

A.0.3 Calculation method for classifying respondents

The classification can be split into three different categories, Fundamentalist, unconcerned, and pragmatist. The classification method can be found in Kumaraguru & Cranor [2005]. The method to group the respondents to each are as follows:

The respondent is grouped into the Privacy Fundamentalists if they have agreed (Strongly or somewhat) with the first statement and disagreed (strongly or somewhat) with the second and third statements.

The respondent is grouped into the Privacy Unconcerned if they have disagreed (Strongly or somewhat) with the first statement and agreed (strongly or somewhat) with the second and third statements.

The respondent is grouped into the Privacy Pragmatists when the above statements are not accepted. I.e. all other answers that do not align with the two other groupings.

B | Scenarios for the survey study

The first scenario the participant is presented for can be seen in Figure B.1. The second scenario the participant is presented for after they have answered the privacy perception questionnaire can be seen in Figure B.2. They both have an introduction that explains how a smart speaker works and the scenario it self, with the minor change that the first scenario is talking to a friend and the second scenario talking to a family member. Furthermore, in scenario 2 there is an added section called Changes which includes how the independent variable is different, as seen in the picture and explain in text how it is different and what to expect from the change. Scenario 1 will always be presented first and scenario 2 presented last as survey tool did not have the option to randomize the conditions. This meant a counterbalancing was not counted for and a carry-over effect might occur during the survey participation. Scenario 2 is a modifyed version of the parasite .

Introduction:

The makers of smart speakers claim that their devices are only activated by specific keywords like "Ok Google". This would mean that they only recognize spoken language after activation. However, the microphones of the smart speaker are always active in order to listen for the spoken commando, like "Ok Google".

Scenario 1

Imagine you are talking to a friend while having a smart speaker in the same room, see picture below for reference.
The context of the conversation is that you are telling your friend that you might have been infected with HIV and are waiting for the final lab results.

Click next when you have understood the scenario.

PREVIOUS NEXT

28%

Figur B.1: Scenario 1. Screenshot of the scenario from the survey study.

Introduction:

The makers of smart speakers claim that their devices are only activated by specific keywords like "Ok Google". This would mean that they only recognize spoken language after activation. However, the microphones of the smart speaker are always active in order to listen for the spoken commando, like "Ok Google".

Changes:

This time the smart speaker is covered by a device, which is blocking the microphones completely, and therefore, no spoken language can be detected by the microphones. You can unblock the microphones by pressing a physical button near the device (not shown in the picture). This way the smart speaker will only be able to listen to you when the button has been pressed and thereby unblocking the microphones.

Scenario 2

Imagine you are talking to a family member while having a smart speaker in the same room, see picture below for reference.
The context of the conversation is that you are telling your family member that you might have been infected with HIV and are waiting for the final lab results. The device has been blocking the microphones during your conversation.

Click next when you have understood the scenario.

PREVIOUS NEXT

57%

Figur B.2: Scenario 2. Screenshot of the scenario from the survey study.

C | Survey

The procedure of the survey

The survey begun with a welcome text that introduces the author, the context of the survey and a short outline of the procedure. Following, the participants were presented to the consent format, which was highlighted to increase likelihood of reading it, before proceeding. Next the participants were presented to a privacy awareness scale, which is followed by the first scenario. It explains the scenario with a picture attached. They were then exposed to the privacy perception questionnaire. In order to have the participant reminded about the scenario while answering, the attached picture was always shown on the top of the questionnaire. The questionnaire was split into three pages. The first page contains the first 7 questions, then 6 questions, and lastly the severity construct questions, this was done to not overwhelm the participants with an exaggerated amount of questions on one page. After the participants were finished with the questionnaire the second scenario begins. The same method of showing the questionnaire was used for the second scenario. When finished, they were then asked to answer the modified privacy awareness scale. After this step, they answered the general questions, which contains confirmatory questions, if they felt more privacy with the device attached, their experience in IT security in terms of years if they own or use a smart speaker, country of residence, age, gender, and comment section for feedback of the survey.

Inconsistencies

The shown survey attached to this document is screenshotted from a computer browser's point of view. The mobile version have a different layout, and depending on the browser size the pc version can have a different layout as in being more condensed, therefore as a note, the layout might look different than the displayed survey below.

Below this page, the whole survey to assesses the privacy perception is shown.

Welcome and consent form.
Dear participant,
thank you for taking the time to answer this survey study. I am a master's student in Engineering Psychology at Aalborg University, and I am working on my master's thesis about the privacy perception of digital devices. In this survey, the digital device is going to be represented by a smart speaker in two different scenarios. You do not need to own a smart speaker to complete this survey. Further details about the smart speaker will be explained on the next page.

Please read the following text carefully before proceeding.
The data collected during this study are your entered data. No other data is collected. The data is going to be evaluated, further processed in the course of the study duration, and then published in the project report section at Aalborg University. It will be impossible to trace the source back to you and you will remain anonymous. This study can be terminated at any given time without the need for an explanation and there will be no negative consequences associated with a termination. It is your decision to approve the use and publication of your data. Participating in this study is completely voluntary. You must be 18 years old or above to participate in this study.
By pressing the "Next" button, you give me your consent that I can collect your answers and assess them till the end of the project. You may at any given time during this study withdraw your consent by closing this survey. In that case, all your data will be deleted.

This survey will take approximately 10-15 minutes to complete.

PREVIOUS NEXT 7%

In the following section, you will be presented by questions relating to your overall attitudes to a given context.
Next, you are presented to two scenarios regarding privacy.
Familiarise yourself with the situations and answer the questionnaires following the scenarios.

In order to fully understand the two scenarios, it will shortly be explained what is meant by a smart speaker.
A smart speaker is a device that is able to recognize spoken language by its microphones, is controlled by voice commands, and is connected to the internet. Examples of smart speakers are: Google Home, Amazon Echo, Apple Homepod, etc.

PREVIOUS NEXT 14%

For each of the following statements, how strongly do you agree or disagree?

	Strongly Disagree	Somewhat Disagree	Somewhat Agree	Strongly Agree
Consumers have lost all control over how personal information is collected and used by companies.	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	○	○	○	○

PREVIOUS NEXT

21%

Introduction:
The makers of smart speakers claim that their devices are only activated by specific key-words like "Ok Google". This would mean that they only recognize spoken language after activation. However, the microphones of the smart speaker are always active in order to listen for the spoken commando, like "Ok Google".

Scenario 1

Imagine you are talking to a friend while having a smart speaker in the same room, see picture below for reference.
The context of the conversation is that you are telling your friend that you might have been infected with HIV and are waiting for the final lab results.

Click next when you have understood the scenario.

PREVIOUS NEXT

28%

Scenario 1

Answer the following statements with respect to the scenario. How strongly do you agree or disagree?
You can go back to the scenario, by clicking on the previous button near the bottom left of this window.

	Strongly disagree	Moderately disagree	Mildly disagree	Undecided	Mildly agree	Moderately agree	Strongly agree
I am afraid that the smart speaker will use personal information, revealed in close proximity to it, in an inappropriate way.	○	○	○	○	○	○	○
I believe I can refuse to give my personal information to this smart speaker when I think it is too personal.	○	○	○	○	○	○	○
I am concerned that revealing personal information close to the smart speaker will involve many unexpected problems.	○	○	○	○	○	○	○
I believe I can conceal some information from this smart speaker when I want to.	○	○	○	○	○	○	○
I believe my personal information is accessible only to those authorized to have access.	○	○	○	○	○	○	○
The information is kept anonymous on this smart speaker.	○	○	○	○	○	○	○
I believe that my conversation is monitored by this smart speaker.	○	○	○	○	○	○	○

PREVIOUS NEXT

35%

Scenario 1

Answer the following statements with respect to the scenario. How strongly do you agree or disagree?
You can go back to the scenario, by clicking on the previous button near the bottom left of this window.

	Strongly disagree	Moderately disagree	Mildly disagree	Undecided	Mildly agree	Moderately agree	Strongly agree
I believe my personal information provided to this smart speaker remains confidential.	○	○	○	○	○	○	○
I feel uncomfortable revealing personal information about me close to the smart speaker.	○	○	○	○	○	○	○
I believe that this smart speaker is collecting too much information about me.	○	○	○	○	○	○	○
There will be a high potential for privacy loss revealing personal information close to the smart speaker.	○	○	○	○	○	○	○
I believe I can hide my true identity using this smart speaker.	○	○	○	○	○	○	○
I believe that the smart speaker will obtain information while having it in close proximity when doing other activities.	○	○	○	○	○	○	○

PREVIOUS NEXT

42%

Scenario 1

Answer the following questions with respect to the scenario, from innocuous to extremely devastating.
You can go back to the scenario, by clicking on the previous button near the bottom left of this window.

	Innocuous, harmless (1)	(2)	(3)	(4)	(5)	(6)	Extremely devastating (7)
Assuming that the topic was recorded by the smart speaker, this would be...	○	○	○	○	○	○	○
Assuming that the topic was only recorded by the smart speaker if it were in use, this would be...	○	○	○	○	○	○	○

PREVIOUS NEXT

50%

Introduction:
The makers of smart speakers claim that their devices are only activated by specific key-words like "Ok Google". This would mean that they only recognize spoken language after activation. However, the microphones of the smart speaker are always active in order to listen for the spoken commando, like "Ok Google".

Changes:
This time the smart speaker is covered by a device, which is blocking the microphones completely, and therefore, no spoken language can be detected by the microphones. You can unblock the microphones by pressing a physical button near the device (not shown in the picture). This way the smart speaker will only be able to listen to you when the button has been pressed and thereby unblocking the microphones.

Scenario 2

Imagine you are talking to a family member while having a smart speaker in the same room, see picture below for reference. The context of the conversation is that you are telling your family member that you might have been infected with HIV and are waiting for the final lab results. The device has been blocking the microphones during your conversation.

Click next when you have understood the scenario.

PREVIOUS NEXT

57%

Scenario 2

Answer the following statements with respect to the scenario. How strongly do you agree or disagree?
You can go back to the scenario, by clicking on the previous button near the bottom left of this window.

	Strongly disagree	Moderately disagree	Mildly disagree	Undecided	Mildly agree	Moderately agree	Strongly agree
I am afraid that the smart speaker will use personal information, revealed in close proximity to it, in an inappropriate way.	○	○	○	○	○	○	○
I believe I can refuse to give my personal information to this smart speaker when I think it is too personal.	○	○	○	○	○	○	○
I am concerned that revealing personal information close to the smart speaker will involve many unexpected problems.	○	○	○	○	○	○	○
I believe I can conceal some information from this smart speaker when I want to.	○	○	○	○	○	○	○
I believe my personal information is accessible only to those authorized to have access.	○	○	○	○	○	○	○
The information is kept anonymous on this smart speaker.	○	○	○	○	○	○	○
I believe that my conversation is monitored by this smart speaker.	○	○	○	○	○	○	○

PREVIOUS NEXT

64%

Scenario 2

Answer the following statements with respect to the scenario. How strongly do you agree or disagree?
You can go back to the scenario, by clicking on the previous button near the bottom left of this window.

	Strongly disagree	Moderately disagree	Mildly disagree	Undecided	Mildly agree	Moderately agree	Strongly agree
I believe my personal information provided to this smart speaker remains confidential.	○	○	○	○	○	○	○
I feel uncomfortable revealing personal information about me close to the smart speaker.	○	○	○	○	○	○	○
I believe that this smart speaker is collecting too much information about me.	○	○	○	○	○	○	○
There will be a high potential for privacy loss revealing personal information close to the smart speaker.	○	○	○	○	○	○	○
I believe I can hide my true identity using this smart speaker.	○	○	○	○	○	○	○
I believe that the smart speaker will obtain information while having it in close proximity when doing other activities.	○	○	○	○	○	○	○

PREVIOUS NEXT

71%

Scenario 2

Answer the following questions with respect to the scenario, from innocuous to extremely devastating.
You can go back to the scenario, by clicking on the previous button near the bottom left of this window.

	Innocuous, harmless (1)	(2)	(3)	(4)	(5)	(6)	Extremely devastating (7)
Assuming that the topic was recorded by the smart speaker, this would be...	○	○	○	○	○	○	○
Assuming that the topic was only recorded by the smart speaker if it were in use, this would be...	○	○	○	○	○	○	○

PREVIOUS NEXT

78%

The scenarios are now over.
You may answer these questions for each of the following statements, how strongly do you agree or disagree?

	Strongly Disagree	Somewhat Disagree	Somewhat Agree	Strongly Agree
Today consumer privacy is sufficiently protected by existing laws and organizational practices.	○	○	○	○
Companies have taken control over how the personal information of consumers is collected and used.	○	○	○	○
The collection of the consumers' information is handled by most businesses in a proper and confidential way.	○	○	○	○

PREVIOUS NEXT

85%

General questions

How strongly do you agree or disagree regarding the scenarios

	Strongly disagree	Moderately disagree	Mildly disagree	Undecided	Mildly agree	Moderately agree	Strongly agree
I felt the conversational information was better protected when the device was attached to the smart speaker.	○	○	○	○	○	○	○
I felt i had less privacy when the device was attached to the smart speaker.	○	○	○	○	○	○	○

How many years have you been working in the field of IT security, e.g., as a student, researcher or practitioner?

-- Choose --

Country of residence

Do you own or use a smart speaker?

- ○ Yes
- ○ No

Age

Gender

- ○ Male
- ○ Female
- ○ Other

If you have any feedback for the questionnaire, you may leave them here.

PREVIOUS NEXT

92%

The end
Thank you so much for your participation!
Your answers have been saved and you can now close the survey.

PREVIOUS FINISH

100%

D | Distribution location and text

Title:

Privacy perception - Spørgeskemaundersøgelse

Danish distribution text for the survey:

Davs! Jeg er en master studerende på Aalborg Universitet. Jeg har til fokus at skrive omkring ens privacy perception i henhold til digitale enheder. I denne spørgeskemaundersøgelse tager jeg udgangspunkt i en smart speaker iht. to scenarier. Man behøver ikke at eje en smart speaker for at kunne deltage og detaljer vil fremstå i undersøgelsen. Det eneste krav er at man er over 18 år gammel. Jeg vil være meget taknemmelig over for din besvarelse!

https://www.survey-xact.dk/LinkCollector?key=XDMWLZQKJ512

Spørgeskemaundersøgelsen tager mellem 10-15 minutter at gennemføre og den er på engelsk.

Mange tak på forhånd!

Distrubted to:

https://www.hardwareonline.dk/

Title:

Privacy perception for a digital device (18+)

English distribution text for the survey:

Hello everyone!

I am a master's student in Engineering Psychology at Aalborg University, and I am working on my master's thesis about the privacy perception of digital devices. This survey is based on two scenarios with a digital device, in this case, a smart speaker. You do not need to own or use one to participate, details will be included in the survey. The only requirement is that you are 18 years old or above. This survey will take approximately 10-15 minutes to complete. I would really appreciate your answers! Thank you, a lot, for your help.

https://www.survey-xact.dk/LinkCollector?key=XDMWLZQKJ512

Distrubted to:

https://reddit.com/r/SampleSize/

Facebook group called: (AAU: Søg, find og bliv testperson)
https://www.facebook.com/groups/715029768587785/

E | Survey data

This appendix includes all data from the Survey.

E.1 Characteristics

The characteristics for the respondents can be seen in Table E.1.

Respondents characteristics (N = 46)	%	#
Gender		
Male	41,3	19
Female	54,3	25
Other	4,3	2
Experience		
No experience	65,2	30
1 year or less	2,2	1
2 years	6,5	3
3 years	2,2	1
4 years	2,2	1
5 years or more	21,7	10
Have or use a smart speaker		
Yes	21,7	10
No	78,3	36
Country of residence		
Denmark	76,1	35
United states	8,7	4
Germany	6,5	3
Finland	4,3	2
Italy	2,2	1
Poland	2,2	1

Tabel E.1: Characteristics of the respondents.

E.2 Extraction of factors

The parallel analysis was done with the help of a web-service that can output a parallel analysis based on, the number of variables, sample size, type of analysis, number of random correlation matrices, percentile of eigenvalues and seed number Gonzaga [2016]. The following data was used to be calculated; Number of variables: 13, sample size: 46, type of analysis: principal components, number of random correlation matrices: 100, percentile of eigenvalues: 95, and seed: 1005. The parallel analysis can be seen in Table E.2

Component or Factor	**Mean Eigenvalue**	**Percentile Eigenvalue**
1	2.025188	2.239414
2	1.721368	1.914565
3	1.49859	1.637769
4	1.330087	1.462013
5	1.183109	1.287914
6	1.040668	1.128458
7	0.922145	1.00318

Tabel E.2: Parallel analysis computed with the help of Gonzaga [2016].

The variance explained by the use of extraction method of principal component analysis can be seen in Table E.3, using data from Raw_Data of condition 1.

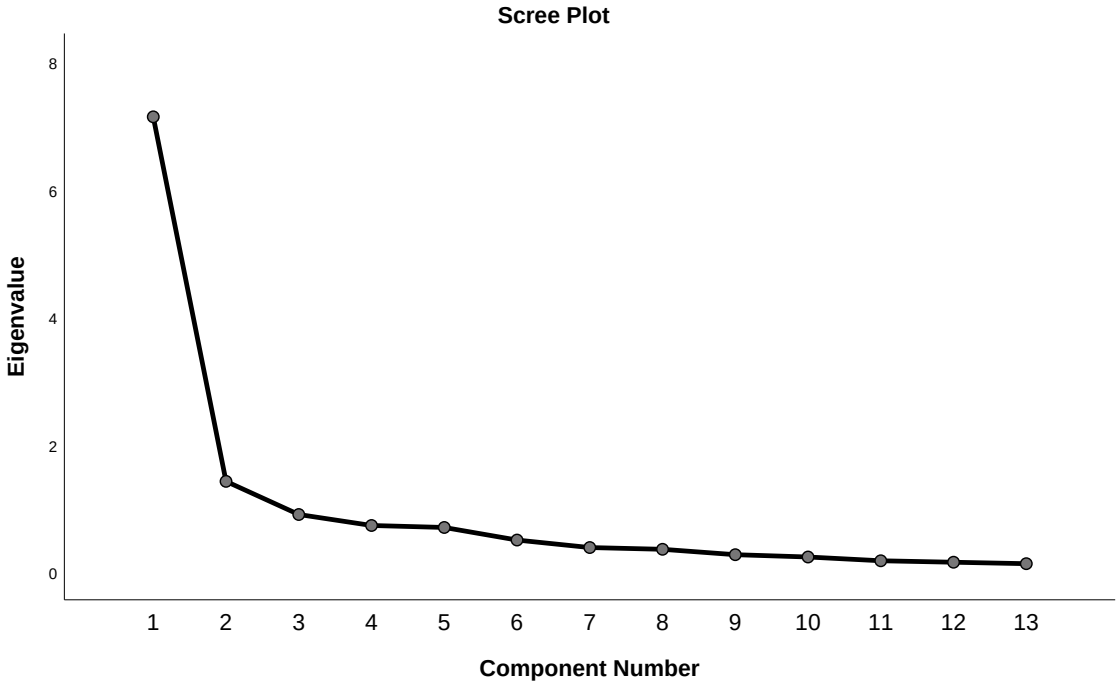
Initial Eigenvalues			
Component	Total	% of Variance	Cumulative %
1	7.136	54.893	54.893
2	1.414	10.880	65.774
3	.894	6.878	72.652
4	.722	5.552	78.204
5	.691	5.313	83.517

Tabel E.3: Initial eigenvalues from extraction method of PCA of condition 1.

The mean eigenvalue from Table E.2 have to be less than the calculated value in row Total of Table E.3 in order to accept the factor. Factor one is less than the mean eigenvalue from the parallel analysis ($7.136 > 2.025$), whereas factor two has a greater mean eigenvalue than from the calculated factor ($1.414 < 1.721$). This means one factor has to be extracted by comparing the calculated values to the parallel analysis and explains 54.89% of the variance.

Other methods of interpretation

Other methods of cut-of can be used by extracting factors with an eigenvalue above 1, or by looking at a scree plot, which is the visualisation between eigenvalues and factors. A scree plot can be seen at Figure E.1. As it can be seen, this indicates factor 1 load huge amount of the variance, and by using the elbow, method for interpretation of the scree plot, it may seem to have two factors.

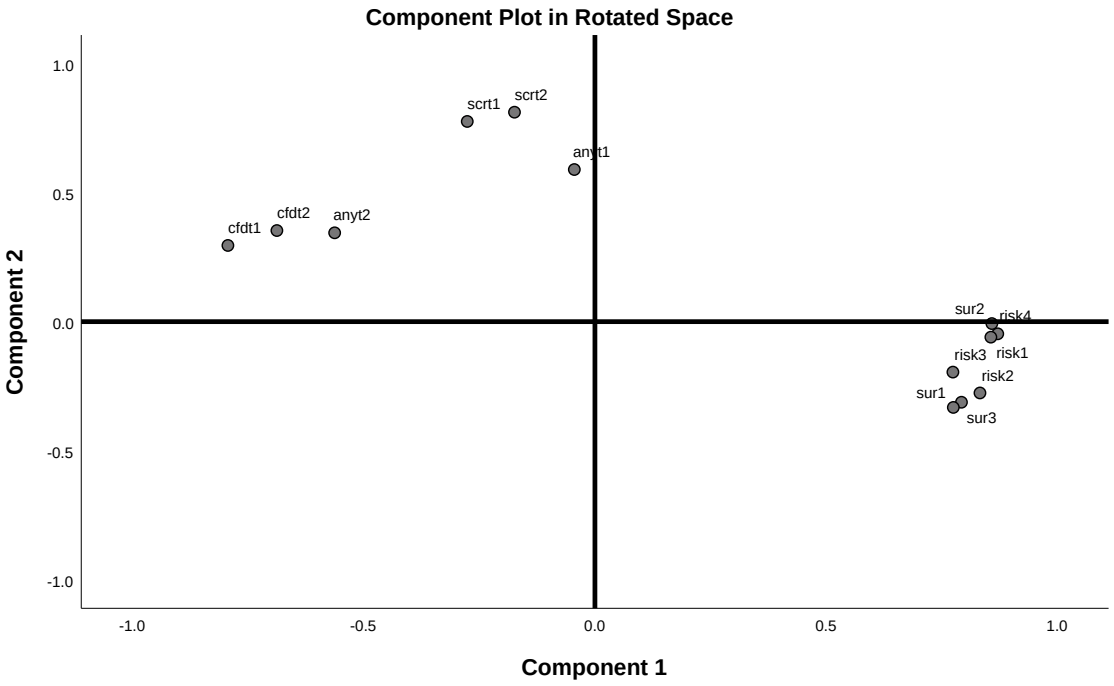


Figur E.1: Scree plot of condition 1.

Assuming it may have two factors, a visualisation of PCA between these two components is made and rotated using Verimax, as the data is orthogonal, see Figure E.2. It can be seen, that all the underlying constructs for perceived privacy control are negative correlated, from affect and surveillance construct. All the affect and surveillance items are group together which has a high loading on component 1. Whereas cfd1, cfd2 and anyt2 are negative correlated with a high loading on component 1. On component 2, scrt1, scrt2 and any1 seem to be loading on component 2. The values of the loading are shown in Table E.4. Furthermore, this proves that all the items for perceived privacy control are negatively correlated, which prompts the solution to reverse code all the items for in construct of affect and surveillance.

Rotated component matrix		
	Component	
	1	2
risk3	.774	-.196
scrt2	-.174	.812
risk4	.871	-.047
scrt1	-.276	.776
cfdt2	-.688	.353
anyt2	-.563	.344
sur3	.793	-.312
cfdt1	-.794	.295
risk1	.856	-.060
sur2	.859	-.007
risk2	.833	-.276
anyt1	-.045	.590
sur1	.775	-.332

Tabel E.4: Rotated component matrix for condition 1, for two components.



Figur E.2: Principal component analysis plot for condition 1.

E.3 Descriptive statistics for conditions

Descriptive statistics for each item after reverse coding for condition 1 can be seen in Table E.5 and for condition 2 in Table E.6. It can be seen that all items have an increased mean from condition 1 to condition 2. A visual representation for the descriptive data can

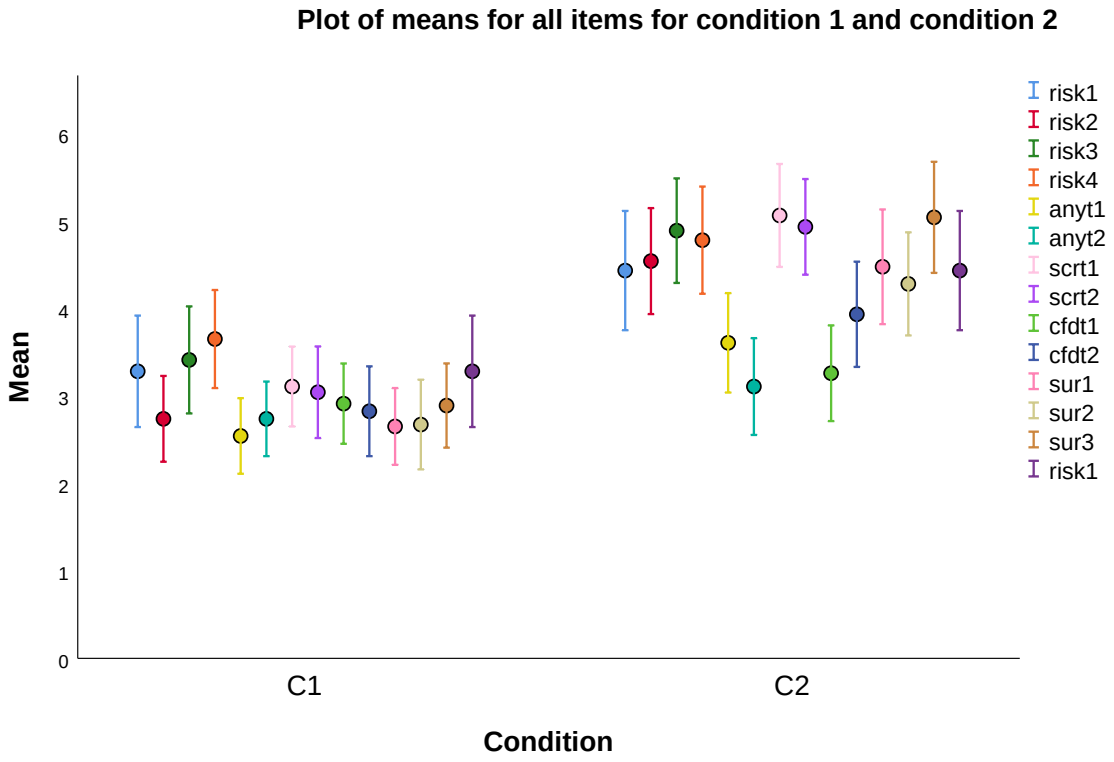
be seen at Figure E.3, with a confidence interval of 95%. For condition 1, it seems that all the data more compact than for condition 2, where anyt1, anyt2, and cfdt1 scores low values, compared to the rest of the items for condition 2.

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
risk1	46	1	7	3.28	2.146
risk2	46	1	7	2.74	1.652
risk3	46	1	7	3.41	2.061
risk4	46	1	7	3.65	1.888
anyt1	46	1	7	2.54	1.456
anyt2	46	1	6	2.74	1.437
scrt1	46	1	6	3.11	1.538
scrt2	46	1	7	3.04	1.763
cfdt1	46	1	7	2.91	1.547
cfdt2	46	1	7	2.83	1.730
sur1	46	1	7	2.65	1.479
sur2	46	1	7	2.67	1.726
sur3	46	1	6	2.89	1.622

Tabel E.5: Descriptive statistics for all questionnaire questions in condition 1.

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
risk1x	46	1	7	4.43	2.296
risk2x	46	1	7	4.54	2.041
risk3x	46	1	7	4.89	2.014
risk4x	46	1	7	4.78	2.065
anyt1x	46	1	7	3.61	1.915
anyt2x	46	1	7	3.11	1.865
scrt1x	46	1	7	5.07	1.982
scrt2x	46	1	7	4.93	1.843
cfdt1x	46	1	7	3.26	1.843
cfdt2x	46	1	7	3.93	2.027
sur1x	46	1	7	4.48	2.208
sur2x	46	1	7	4.28	1.985
sur3x	46	1	7	5.04	2.139

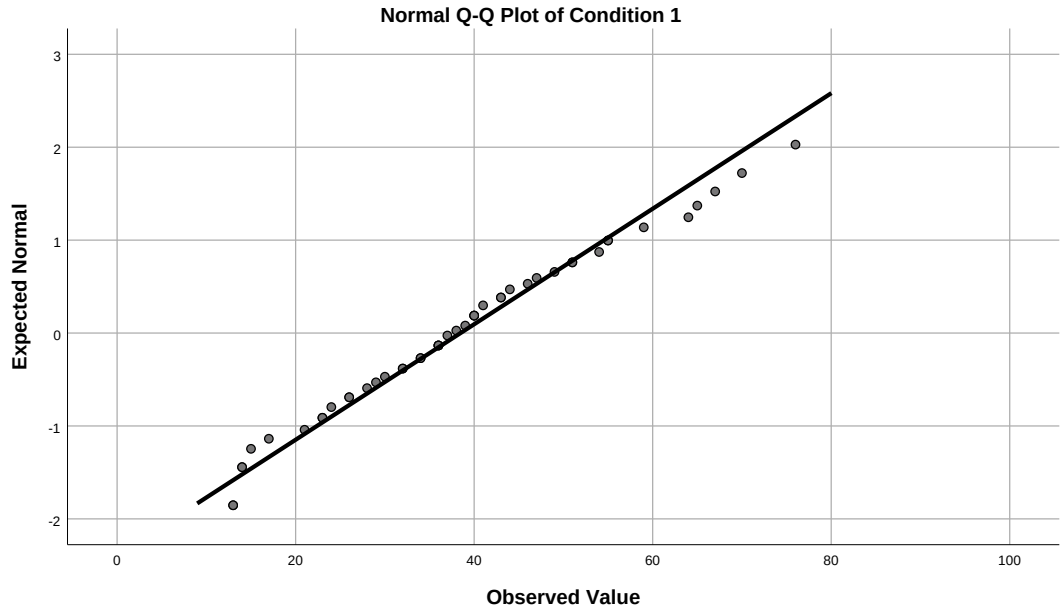
Tabel E.6: Descriptive statistics for all questionnaire questions in condition 2.



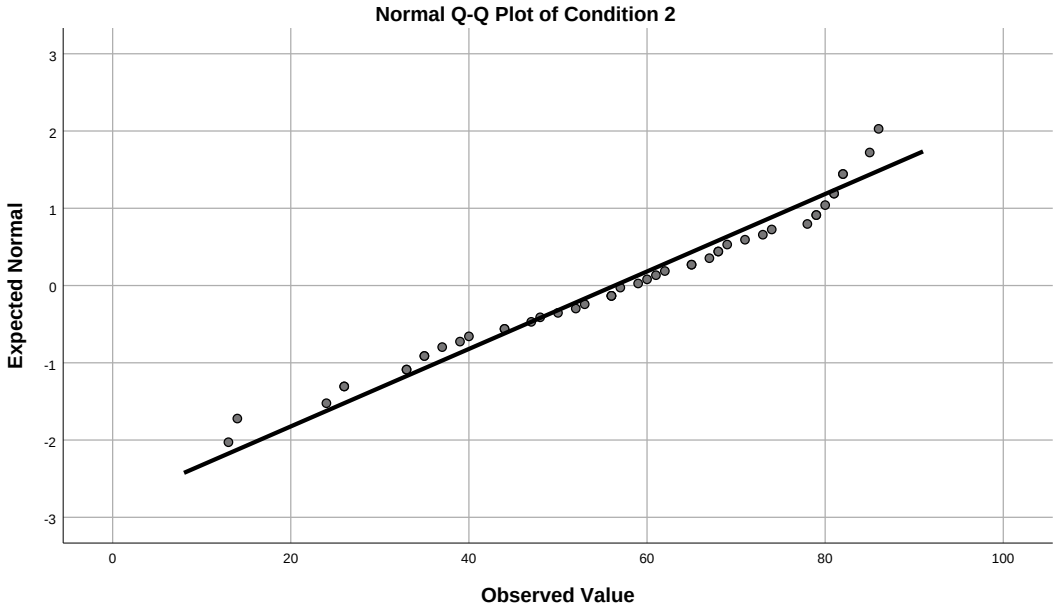
Figur E.3: Plot of means for all items of both conditions (C1 and C2). These are included with error bars of 95% confidence interval.

E.4 Test for normality

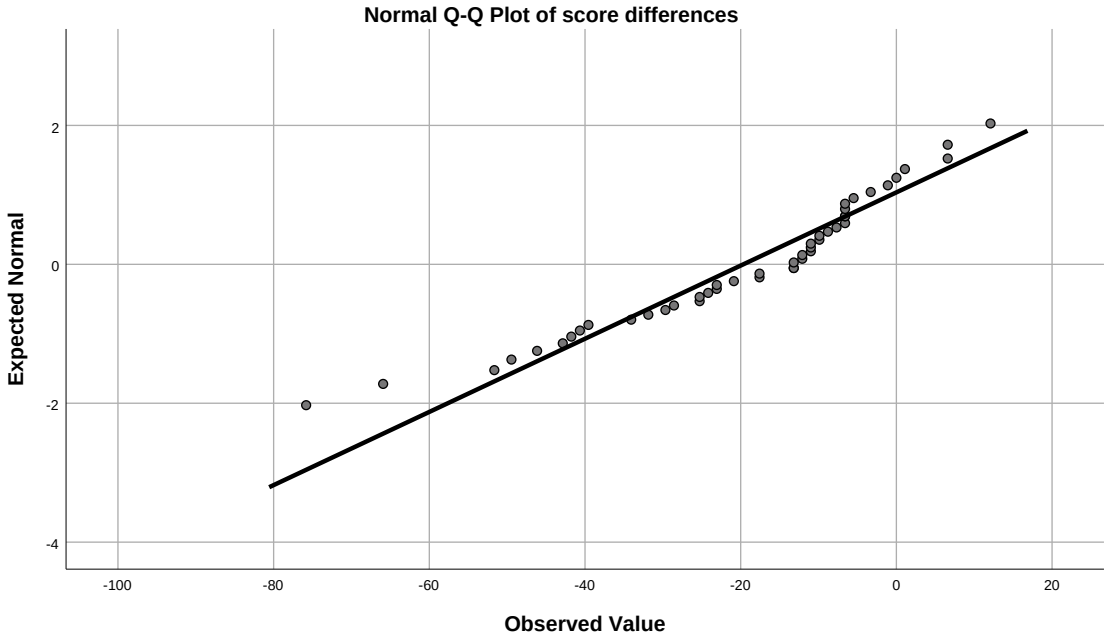
When testing for normality an assumption of having a normal distribution for the sample is required in order to use parametric tests. A visual representation can be seen for condition 1 at Figure E.4 and Figure E.5. They both seem to follow the diagonal line, and therefore normal distributed. The test scores for normality Shapiro-wilks test is used. Both conditions do not reject the null hypothesis, condition 1 $W(46) = 0.972$, $p = .34$ and condition 2 has $W(46) = 0.957$, $p = .084$, therefore the test concludes that they are normal distributed. Paired sample t-test is a parametric statistical method to measure difference between two dependent variables in a repeated measure experiment. The assumption test that is needed is to test for normality and outliers. The data that has to be used is the difference between condition 1 and condition 2 scores. In other words, condition 2 - condition 1 = difference. The difference reject the null hypothesis, $W(46 = 0.933)$, $p = .010$. The difference is not normally distributed according to Shapiro-Wilk's normality test. The visual Q-Q plot of differences can be seen at Figure E.6. It seems to follow the diagonal line. When inspecting the skewness, a score of 0.963 with SD of 0.350 which gives a Z-score of 2.7. The acceptable Z-score range is between -1.96 and 1.96 [Kim, 2013]. This means that the difference between the condition can be considered positively skewed and not normality distributed.



Figur E.4: Q-Q plot for condition 1. Normal distribution values compared to scored values of condition 1.



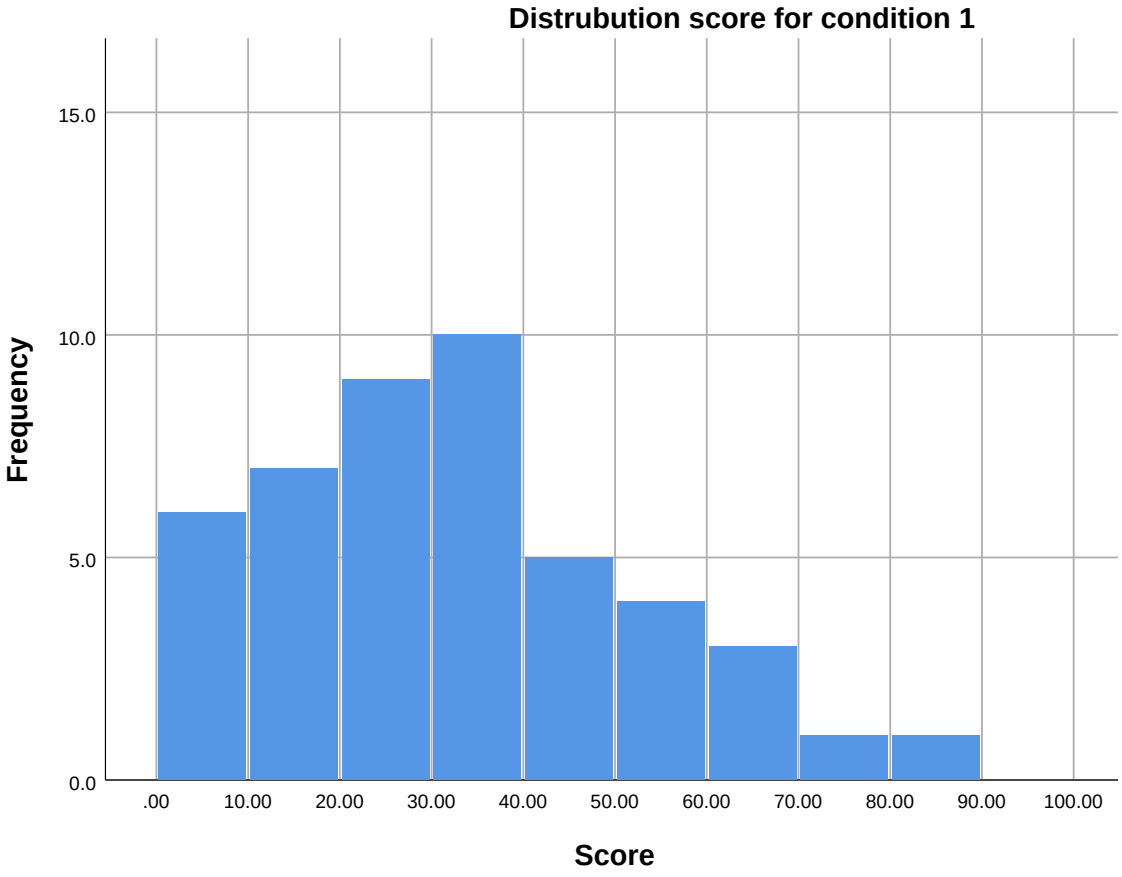
Figur E.5: Q-Q plot for condition 2. Normal distribution values compared to scored values of condition 2.



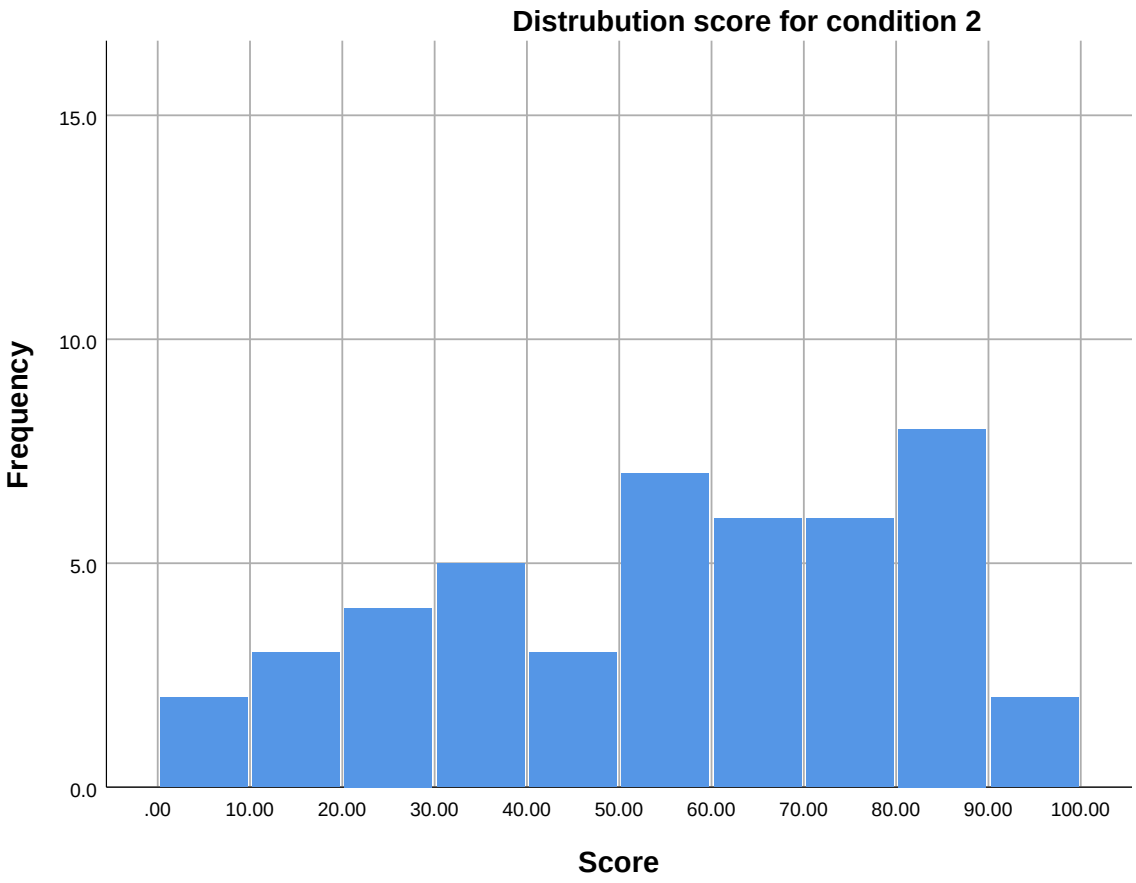
Figur E.6: Q-Q plot for difference of condition 1 and 2.

E.5 Data distribution

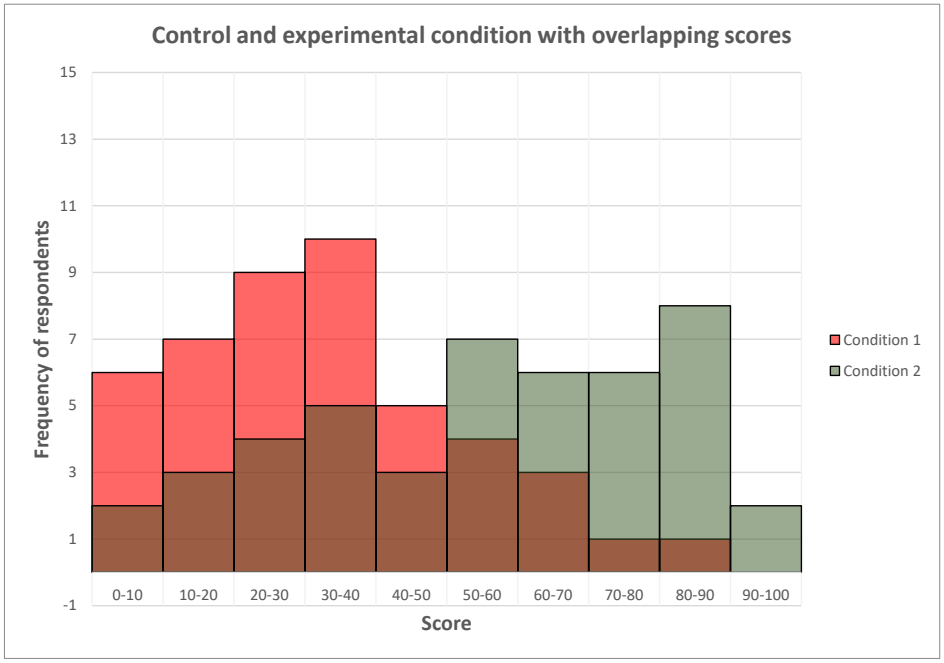
The data that have been used for this section is the standardized data. This data ranges from 0 to 100 after the method of scoring have been applied as seen in Digital Appendix Section F.2. The distribution of the scored data for condition 1 ($M = 32.66$, $SD = 20.63$), can be seen in Figure E.7. The distribution of the scored data for condition 2 ($M = 55.60$, $SD = 25.57$), can be seen in Figure E.8. The distribution for each condition can be seen overlapped at Figure E.9. The difference between the paired values of condition 1 and condition 2 can be seen at Figure E.10 ($M = 22.94$, $SD = 22.15$). The pairwise differences for each of the respondents shows most respondents answers in favor of condition 2 as being perceived as having more privacy. Few respondents had extreme responds as in low privacy perception for condition 1 and high privacy for condition 2.



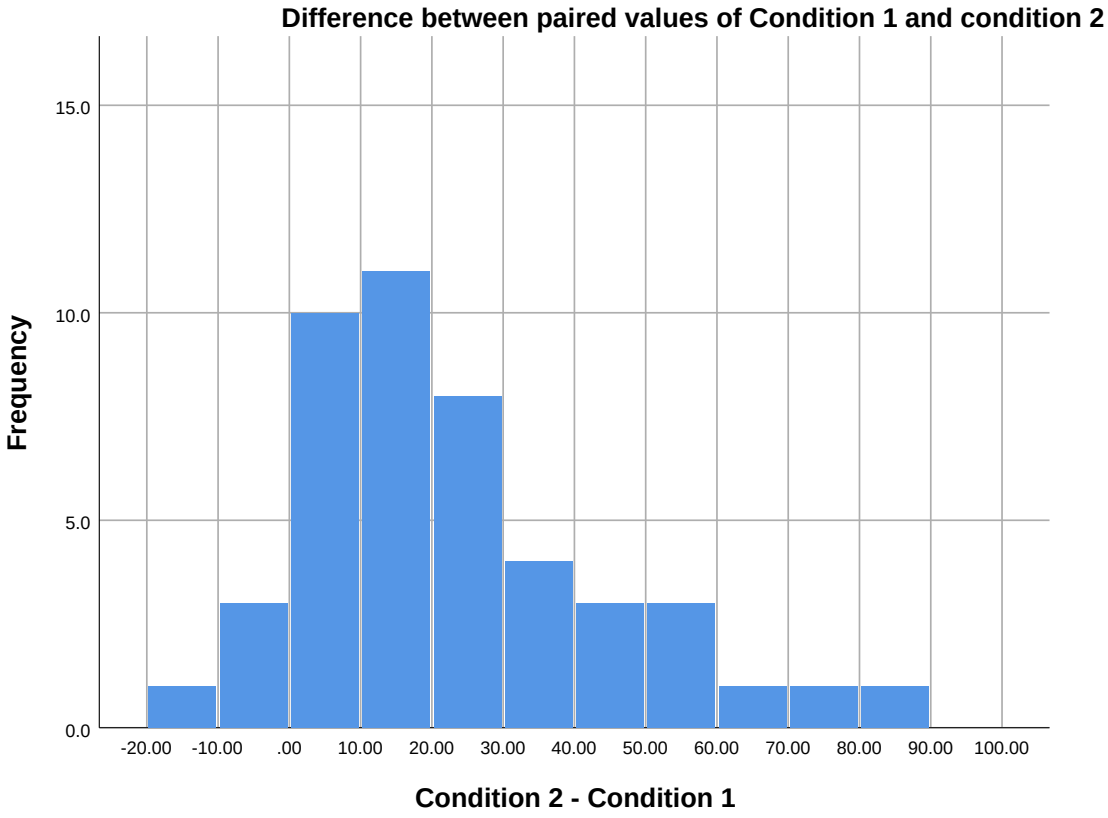
Figur E.7: Distribution score for condition 1.



Figur E.8: Distribution score for condition 2.



Figur E.9: Privacy perception summed scores for control condition 1 and experimental condition 2.

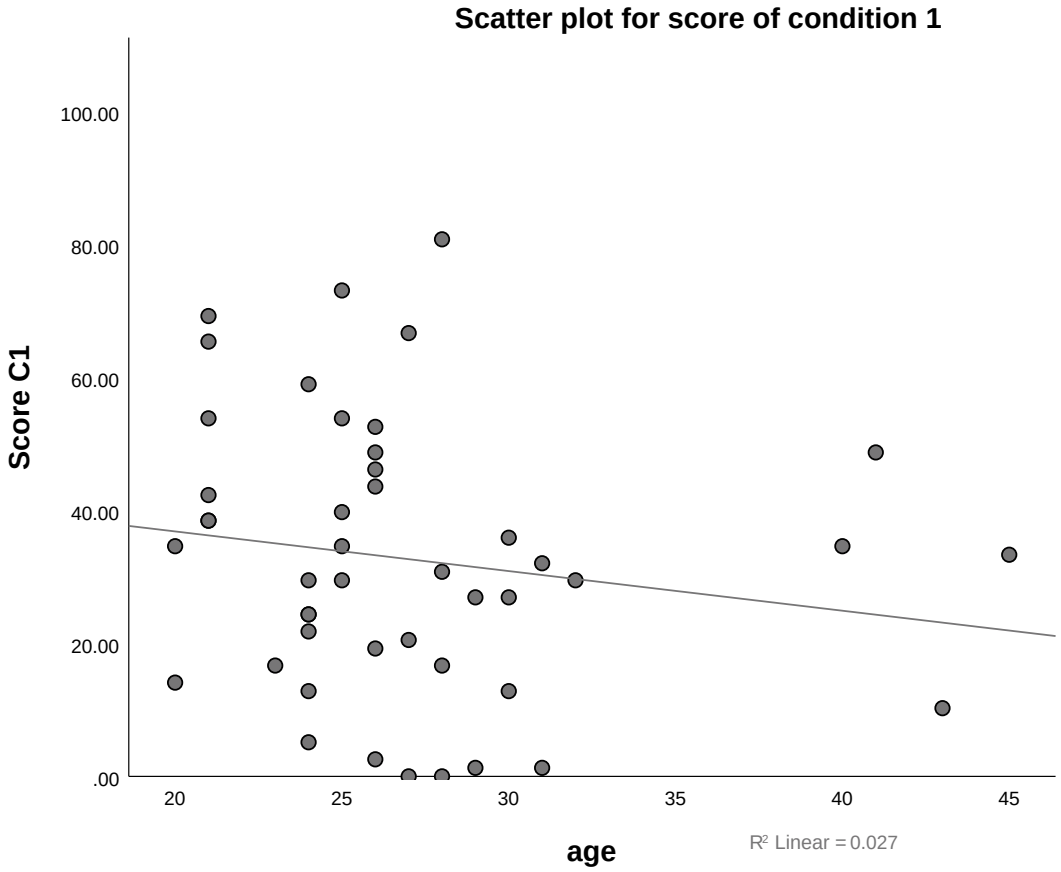


Figur E.10: Difference between condition 2 and condition 1 of the paired values.

E.6 Check for confounding factors

Age

In order to check if there is a correlation between age and the score, Spearman's correlation can be used. This assumes that the scatter plot between the two ordinal or continuous variables have a monotonic relationship. As seen in Figure E.11, this assumption is not meet, and therefore can not be computed. From the scatter plot, it seems that there is no relationship between age and score.

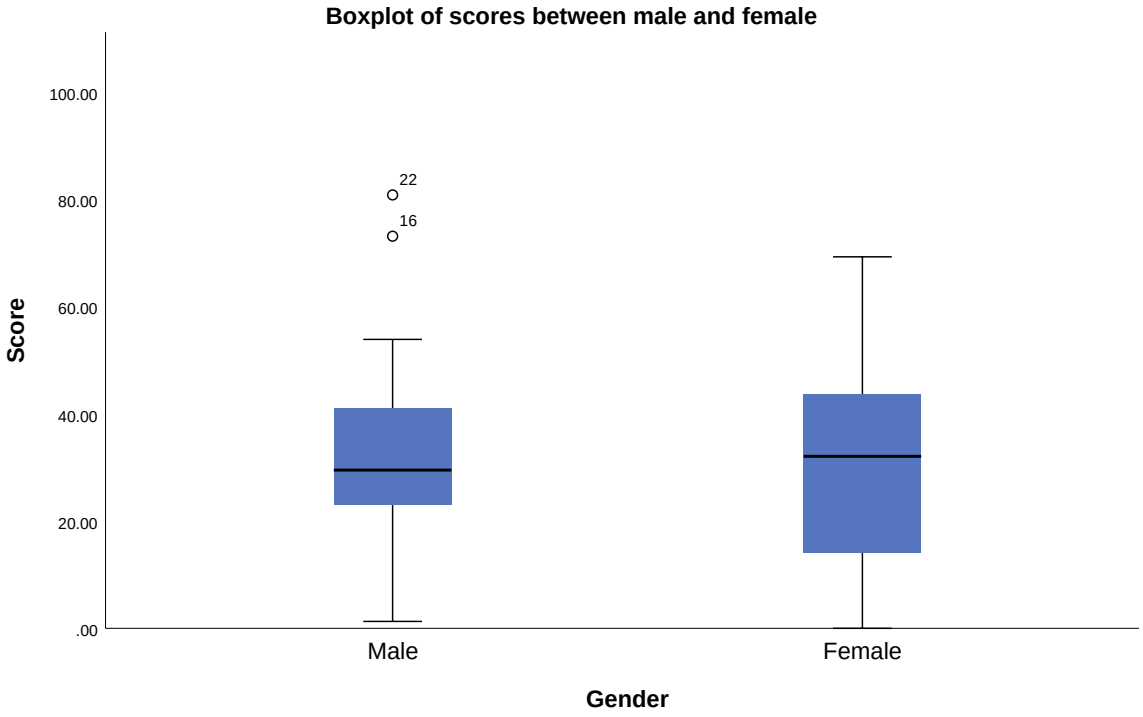


Figur E.11: Scatter plot between age and score for condition 1.

Gender

It was chosen to remove the gender item called other, as there only were two people in this group. In order to use a parametric test for gender, a Shapiro-wilk test for normality is used. Privacy scores for both genders were normally distributed, assessed by Shapiro-wilk's test ($p > .05$). When checking for outliers, a boxplot can be presented, as seen in Figure E.12. It shows two outliers, respondent 22 and 16. It is chosen not to modify or remove the outliers, because the measurement is indeed subjective, and these two respondents may have a feeling of more privacy than the rest of the male sample. Therefore a parametric test is not

used, and instead a non-parametric is used. A Mann-Whitney U test was run to determine if there were difference in privacy score between male and female. The distribution between male and female were similar, as assess by a visual inspection. Privacy score for condition 1 were not significant between males (Mdn = 29.49) and females (Mdn = 32.05), U = 236.5, Z = -.024, p = .981.

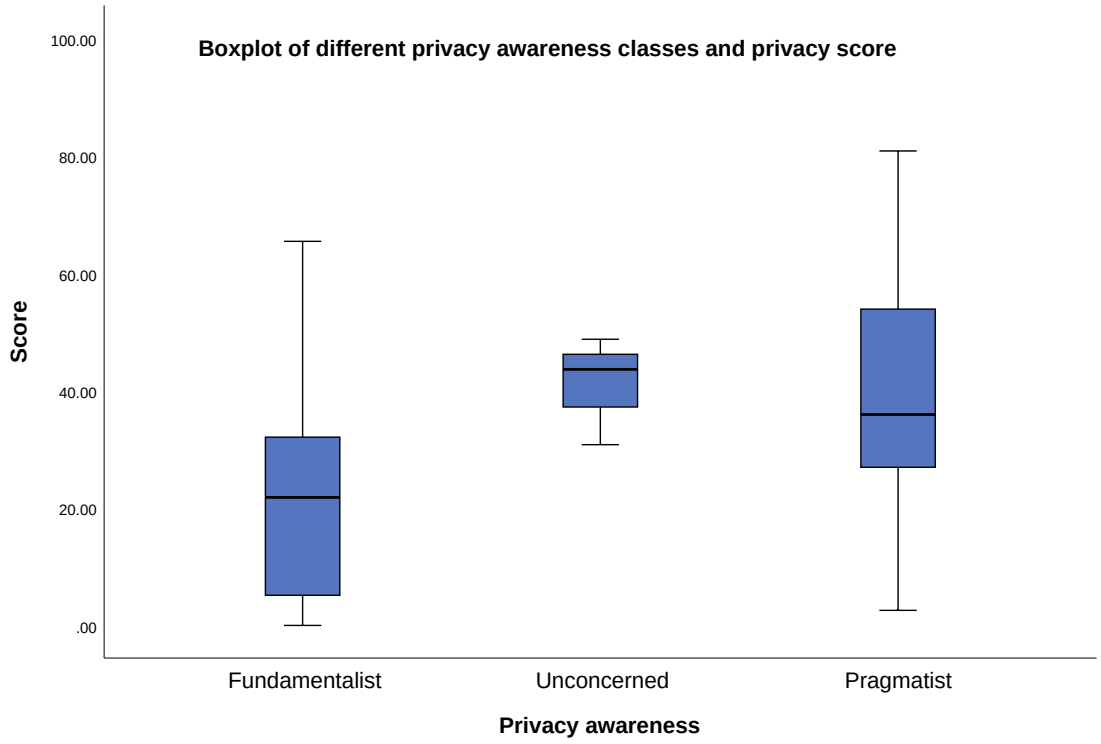


Figur E.12: Boxplot of gender and score for condition 1.

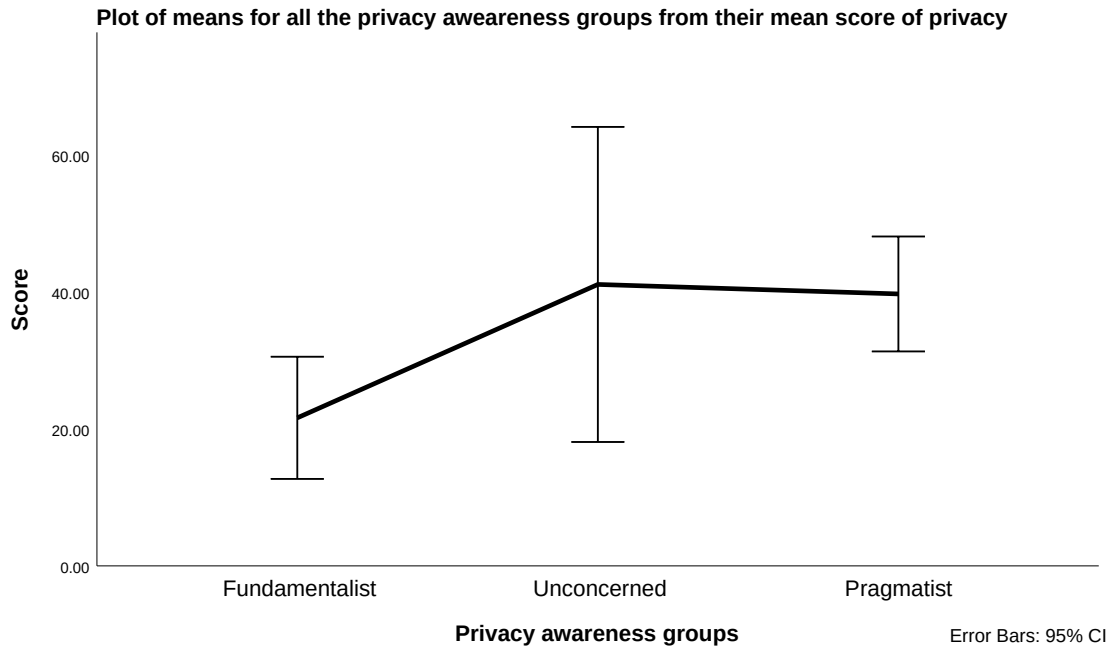
Privacy awareness

To check if the groups between of privacy awareness (fundamentalist, unconcerned, and pragmatist) have an influence on privacy scores, a parametric test in this case one-way ANOVA is used of the results from the first privacy awareness score and privacy score. Firstly, checking for outliers, there were no outliers in the data, as assessed by an inspection of a boxplot, see Figure E.13. Privacy score was normally distributed between all groups, as assessed by Shapiro-Wilk's test ($p > .05$). To test for homogeneity of variance, Levene's test is used. There was found homogeneity of variance, as assessed by Levene's test for equality of variances (p = .354). The privacy score were lowest for fundamentalist (n = 18, M = 21.58, SD = 17.91), whereas pragmatist (n = 25, M = 39.64, SD = 20.29) and unconcerned (n = 3, M = 41.02, SD = 9.25), had a relatively same mean between each other and higher mean than fundamentalist. A visual representation of the difference between the group means can be seen at Figure E.14, with error bars of 95% confidence interval. One-way ANOVA was performed to see if there is a difference between the groups, it can be assessed that there was a statistically significant difference in privacy awareness classification groups and privacy scores, $F(2, 43) = 5.044$, $p < 0.011$, $\eta^2 = .190$ As the

ANOVA shows there is a difference, this difference is to be found. Tukey post hoc test can be used as homogeneity of variance is not violated in order to find between which group this difference lies, however, the group sizes between each class is not equal and therefore a modified test have to be used, in this case Tukey-Kramer post hoc test. Tukey post hoc analysis revealed a mean increase from fundamentalist to pragmatist (18.06, 95% CI[3.8, 32.31]) was statistically significant ($p = 0.10$), no other group difference were statistically significant.



Figur E.13: Boxplot of privacy awareness classes and score for condition 1.



Figur E.14: Plot of means between each of the groups from privacy awareness of their mean score of privacy perception for condition 1.

F | Table of contents for digital appendix

F.1 Scale editing

F.2 SurveyData

Classifying

Score

Raw_data

All_data_reverse_Coded