Nudge me correctly

Social proof and reciprocity nudges and the online privacy protection behavior of Generation X and Generation Y

Author:	Sanne H. Nijland
Student Number:	s2205483
Course:	Master Thesis
Main supervisor:	J.J van Hoof
Education:	Master Communication Studies
Date:	December 14, 2020
Word count:	18,554

Nudge me correctly

Social proof and reciprocity nudges and the online privacy protection behavior of Generation X and Generation Y

Author:	Sanne H. Nijland
Student number:	s2205483
Education:	Master Communication Studies
Specialization:	Digital Marketing Communication
Institution:	University of Twente
First supervisor:	J.J. van Hoof
Second supervisor:	M. Galetzka
Date:	December 14, 2020

Acknowledgements

This thesis is the final challenge of the Master Communication Studies at the University of Twente. In this thesis I focused on the online context because of my specialization in Digital Marketing Communication and my interest in this field. Moreover, I have chosen a topic that is very topical at the moment. During my thesis, the coronavirus broke out in all parts of the world. My thesis investigates online privacy protection behavior in the environment of a fictional corona-app. I considered it a very interesting process from which I learned a lot. In addition to applying my acquired knowledge and skills from the Master, I have grown as a person. Due to the coronavirus, it was a difficult period to write my Master Thesis. This is because all communication lines were longer than under normal circumstances. This applies to both the communication with my supervisors and the communication with participants in the preliminary research. I found it more difficult to convey information in this impersonal way. I had to learn to deal with this during this process and it taught me how to convey information even better to someone.

I want to express my gratitude to my first supervisor, dr. J.J. van Hoof, for his time, help, advice and feedback during this whole challenge. Further, I would like to thank my second supervisor, dr. M. Galetzka, for her time, advice and feedback that helped me to complete my thesis. The feedback sessions together with my two supervisors kept me thinking and rethinking throughout the process. Succeeding this final challenge could not have been accomplished without their help.

In addition, I would like to thank the participants in this study. All participants in the preliminarily research and experiment took the time and effort to participate. Their help is much appreciated and has led to new insights. Without their help, I could not have conducted this research.

Abstract

Purpose: Generation X and Generation Y both show high online privacy protection behavior due to their online privacy concerns. Therefore, this study focuses on the online privacy context. Currently, nudges are mainly being implemented for the average person in a certain group of people, but there is no further segmentation within this group. Generation segments can be used to target different generations, each with their specific behavior and needs. Therefore, this study investigates the influence of online nudges on the online privacy protection behavior of Generation X and Generation Y.

Methodology: The hypotheses of the study were tested with an experiment, involving Generation X and Generation Y participants, using nudges in a privacy notification in a fictional corona-app interface. The study contained a 2x2 between-subjects experimental design. The experimental manipulations differ from each other by nudges; social proof nudge (yes/no) and reciprocity nudge (yes/no), influencing the online privacy protection behavior in the fictional corona-app. In addition, questions were asked about participants' level of familiarity, uncertainty, and quick decision regarding the corona-app (CoronaMelder).

Results: Generation X and Generation Y both showed online privacy protection behavior. Both generations showed approximately the same online privacy protection behavior in the fictional corona-app, but Generation X showed more online privacy protection behavior on the internet than Generation Y. Moreover, the results showed that the nudges had no effect on the online privacy protection behavior and they had no different effect on generations. Moreover, the nudges were not strengthened or weakened by familiarity, uncertainty and quick decision.

Conclusion: The social proof nudge and reciprocity nudge had no different effect on the online privacy protection behavior of Generation X and Generation Y. However, the study showed some interesting outcomes that were not expected; participants with a high level of familiarity and quick decision, plus a low level of uncertainty regarding the fictional corona-app, showed less online privacy protection behavior.

Keywords: digital nudging, social proof nudge, reciprocity nudge, generation x, generation y, online privacy protection behavior

Table of contents

1. Introduction

Nowadays, nudges are being implemented in many different contexts in order to improve people's decisions. According to Thaler and Sunstein (2008), nudges are changes in the choice architecture that predictably influence decisions people make without restricting their freedom of choice. Furthermore, nudges are activities that change people's behavior by 'nudging' them into a desirable direction where low costs and minimum efforts are being made. For example, nudges in cafeterias can prompt people to choose a healthy food option instead of an unhealthy food option from a menu. This was achieved by placing the healthy option at eye level, making it easier to reach. However, the unhealthy option was not removed from the menu, it was still available, but the ability to reach it was more difficult than for the healthy option (Thaler & Sunstein, 2008).

Studies currently focus on identifying nudges that have an effect on, as Peer et al. (2019) call it, "the average level of people in general" (p. 3). This means that a nudge is targeted to the 'average person' in a certain group of people (such as the 'average consumer'), but that there is no further segmentation within this group. Nudging the average person may lead to suboptimal results because the possibility is that a nudge can have a strong effect on some people but a smaller or negative effect on others, for whom another nudge may be more effective. Nudges are aimed at changing the behavior of the 'average' consumer. Therefore, targeting specific nudges to subpopulations is an important problem that remains unresolved (Peer et al., 2019).

Consumers can be divided into different segment categories such as demographic, lifestyle and purchase intention segments. Another segment category is the generation segment. Generation segments can be used to target different generations, each with their specific behavior and needs (AudienceData, 2018). Generations came from a different background and that is why they have different coping skills and expectations (Reisenwitz & Lyer, 2009). However, not much is known about targeting nudges to generation segments. This is one important gap that this study aims to fill in, because it is expected that generations respond differently to nudges and therefore one nudge may work better for one generation while another nudge may work better for another generation. Generation X and Generation Y are taken into account because these generations were born before the popularization of the internet and they are characterized by higher rates of internet adoption, in comparison to older generations (Lissitsa & Kol, 2016).

In 2019 in the Netherlands, Generation X and Generation Y have high online privacy protection behavior because both generations have concerns about their online privacy while using the internet (Ruigrok NetPanel, 2019). Nudges have the potential to reduce their online privacy protection behavior by relieving some of the privacy burden by making it easier for people to make a choice, without restricting their freedom of choice (Acquisti, 2009). People from Generation X were born between 1965 and 1975. Compared to other generations, Generation X reads more reviews and visits more opinion sites to get the reassurance that their choices are right (Wai Kwan Leung & Taylor, 2002; Parelta, 2015). Based on these characteristics of Generation X, the social proof nudge is able to influence this generation. Social proof explains that people rely on social cues from others on how to feel, think and act in situations (Cialdini, 2009). Figure 1 visualizes the core properties of Generation X. In addition, people from Generation Y were born between 1985 and 1995. This generation is also known as 'Generation Me', which means that Generation Y, compared to other generations, is very extrinsic and materialistic, emphasizing money and image (Twenge, 2014). Based on these characteristics of Generation Y, the reciprocity nudge is able to influence this generation. Reciprocity requires people to respond to positive or negative actions with similar actions, thereby repaying the original actions (Cialdini, 2009).

Figure 2 visualizes the core properties of Generation Y. This study uses a social proof nudge and reciprocity nudge to reduce their online privacy protection behavior and disclose their privacy information. While conducting this study, the coronavirus broke out in the Netherlands and other parts of the world and to limit the spread of the virus a 'corona-app' (CoronaMelder) was being developed and tested. The hypotheses of this study are tested in an experiment using a social proof nudge and reciprocity nudge in a privacy notification in a fictional corona-app interface. The study aims to answer the following research question:

"To what extent can social proof and reciprocity nudges influence the online privacy protection behavior of Generation X and Generation Y?".

This study is of theoretical value because it contributes to the existing literature about the influence of social proof and reciprocity nudges on the online privacy protection behavior of Generation X and Generation Y. Moreover, when it comes to future research, several new questions have emerged from this study. In addition, the study is of practical value for the government, social stakeholders, online marketers and entrepreneurs since they can use the insights of the study to change the online privacy protection behavior of Generation X and Generation Y for privacy-related online platforms.

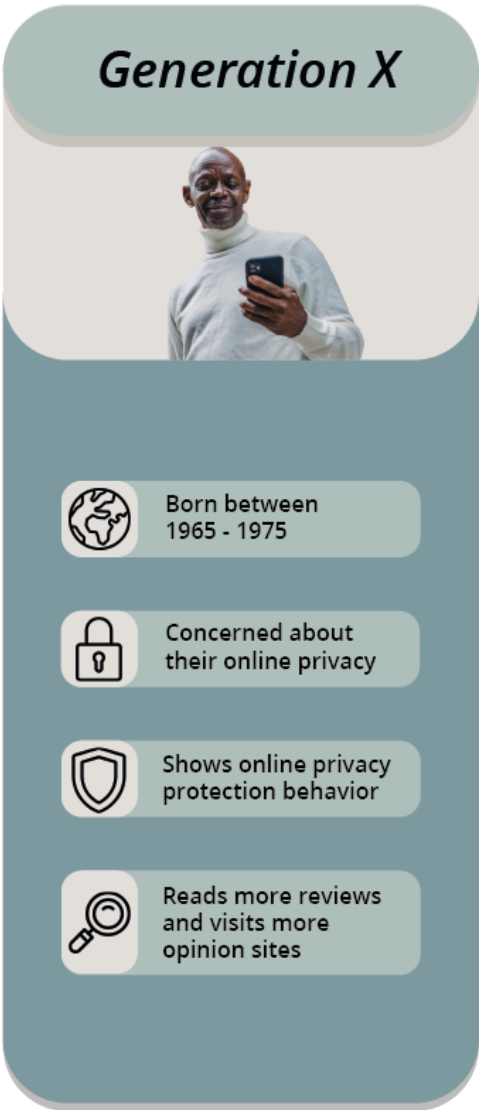

Figure 1. Generation X

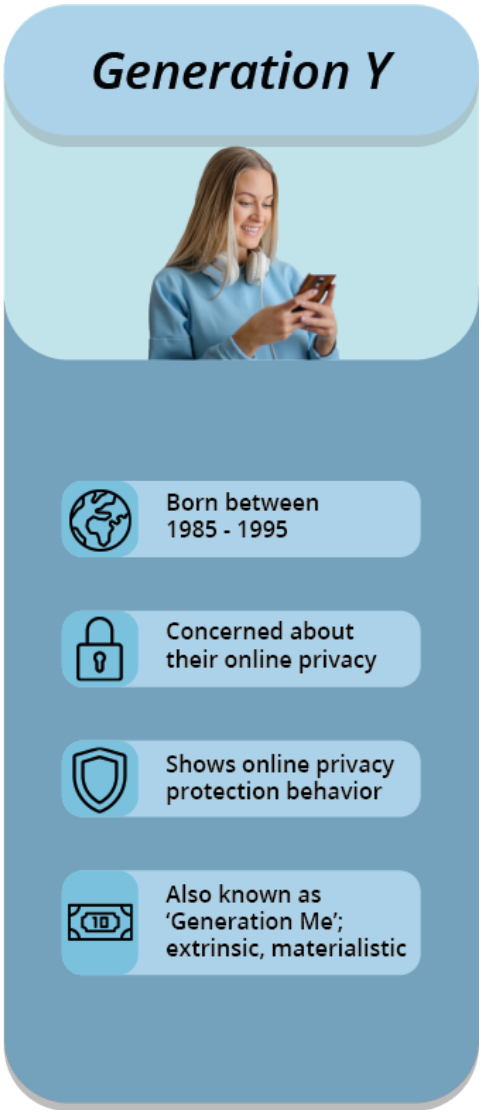

Figure 2. Generation Y

2. Theoretical framework

The theoretical framework describes the online privacy protection behavior, nudges, familiarity, uncertainty, quick decision and generational differences. In addition, this chapter includes the hypotheses of this study based on the literature review and presents the conceptual framework of the study.

2.1. Online privacy protection behavior

In 2019, 52% of Dutch people are concerned about the online security of their personal data and 47% of Dutch people state that they do not feel in control of their online privacy. Moreover, despite the regulation of the GDPR (or AVG in Dutch), 44% of Dutch people think that the Dutch government is not taking sufficient measures to protect their online privacy (Ruigrok NetPanel, 2019). In addition to this research, the research by Autoriteit Persoonsgegevens (2019), in English the Dutch Data Protection Authority (DPA), shows that 94% of Dutch people in 2019 are concerned about the protection of their personal data. Especially in online shops, people are most concerned about the processing of their personal data. The concerns are mainly motivated by the fear that these data will fall into the wrong hands.

It is not surprising that these studies show that many Dutch people are concerned about their online privacy, as today people are faced with an increasing number of privacy decisions during online activities. That is because the internet requires people to disclose personal information online. Personal information is the information that is directly about someone, or can be traced back to a person, such as a person's name, telephone number, location, and health data (Autoriteit Persoongegevens, 2019). In this study people must accept that an app uses their personal data, health data and location data. If people do not want these types of personal information to be used by online platforms or they are concerned about their privacy, they are more likely to engage in protective behavior (Boerman et al., 2018). Protective behavior is defined as "specific computer-based actions that consumers take to keep their information safe" (Milne et al., 2009, p. 450). More specifically in the online privacy context, online privacy protection behavior is the action people take to prevent the unwanted disclosure of their personal information while using the internet (LaRose & Rifon, 2007).

In his research on determinants of online privacy concern and its influence on privacy protection behavior among young adolescents, Youn (2009) investigated the approach and avoidance coping styles to deal with privacy risks and perform online privacy protection behavior. The approach strategies include fabricating personal information and searching for social proof or information. Moreover, avoidance strategies include withholding personal information by refraining. The study showed that people have three different strategies for performing online privacy protection behavior: fabricate, search, and refrain. Fabricate refers to people's efforts to provide incomplete information about themselves. In addition, searching refers to people's efforts to ask other people for advice or to read the privacy statement. Further, refrain represents the refusal of people to use the website that asks them to provide personal information. These three strategies are used in this study to indicate people's online privacy protection behavior.

According to research on the factors influencing individual's behavior on privacy protection, the behavior of young adolescents on privacy protecting is affected by the personal psychological factors and external influences (Hsu & Shih, 2009). The external influences include the environment that affects the person's privacy behavior. In addition, the internal influences are people's beliefs on privacy protection and their privacy concerns.

In this study, the personal psychological factors include people's privacy concerns and privacy protection. Moreover, the nudges in the fictional corona-app interface are a form of external influences. These two privacy factors will be discussed further in the following chapters.

2.2. Nudges

Nudges can be used to influence people's behavior and were introduced by Thaler and Sunstein (2008, p. 6). According to their book, "a nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be cheap and easy to avoid". This intervention can be conducted by presenting choices in such a way that people will select the one they think is most beneficial. The biggest advantage of nudging people is that the possibility of their independent choice is being maintained (Didenko, 2016).

Furthermore, nudges are built on the fact that people do not always make rational and informed choices. Actually, most of the choices people make are done automatically and intuitively. It is difficult to change this impulsive behavior by arguments only. What will work, are small changes in the psychical environment. A subtle hint can have a significant and behavioral effect (Workwire, 2015). A nudge is a subtle way to persuade, it involves passive behavioral change because there is a grip on the automatic behavioral system. It is all about a positive interaction in which no compulsion or punishments are used (Van Kempen, 2017). When a person is being persuaded too coercively, the risk appears that a person finds it aggressive and will not appreciate it, resulting in reactance. However, when a person gets persuaded too lightly, it will get nowhere (Psychology Today, 2018). In their paper about the assessment of the definitional scope of nudges, practical implementation possibilities and their effectiveness, Michalek et al. (2016) assess that nudges would be most effective when they are applied to behavioral situations that are dominated by cognitive processes such as reflexes, making choices under tight time constraints and low involvement decisions.

Nowadays, nudges are being implemented in the online world because the increasing use of digital technologies causes that people often make decisions within digital choice environments. Weinmann, et al. (2016) define digital nudges, also known as online nudges, as "the use of user-interface design elements to guide people's choices or influence user's inputs in online decision environments" (p. 433). Digital nudging works by modifying what is presented (content of choices) and modifying how it is presented (visualization of choices).

Nudges are the external influences which affect people's behavior on protecting their online privacy. According to Acquisti (2009), privacy nudging attempts to relieve some of the privacy burden by making it easier for people to make a choice, without restricting their freedom. People can be 'nudged' to turn them around in ways that do not diminish their freedom but offer them the options of more informed choices. A previous study on nudges for privacy and security by Acquisti et al. (2017) already addressed that nudges can be used to nudge people away from privacy. More specifically, the ease or attractiveness of one option can nudge people toward choosing it. Many existing choices are designed to be the most obvious, smartest or easiest option that can discourage the privacy of information. For example, the option to unsubscribe from promotional emails is in small and neutral colors at the bottom. Another example is a button that you agree to revealing private data which is usually displayed in bright colors, making it more attractive than the other neutral colored button to not reveal the private data. In addition, the button for revealing private data is often placed on the right side of the notification which is a position that is often used for buttons implying forward movement.

2.2.1. Types of nudges

There are several types of nudges that can improve people's decisions. Cialdini (2009) categorized persuasion in six main principles: commitment and consistency, liking, reciprocity, authority, scarcity and social proof. First, commitment and consistency explain that people prefer to be consistent with the things they have previously done or said. The principle of liking explains that people prefer to say yes to those people they like. Authority is the idea that people follow the lead of experts. Moreover, scarcity means that people value what is scarce. Perceived scarcity of an object makes people want it more.

Recently, Cialdini (2017) added a seventh principle, unity, to the main principles of persuasion. Unity is about shared identities. The more we see people as 'we', the more likely we are to be influenced by these people.

Based on the characteristics of Generation X (see Chapter 2.4.2) and Generation Y (see Chapter 2.4.3), this study focuses on the principles of social proof and reciprocity. This chapter therefore explains these two principles in more detail.

Social proof nudge

According to Cialdini (2009) social proof explains that people rely on social cues from others on how to feel, think and act in situations. Therefore, people will do things that they see other people do. They allow themselves to be influenced by the behavior of others, especially in uncertain and unclear situations. More specifically, in situations of uncertainty people draw on social proof as a source of information to get guidance for their own actions. Organizations often use social proof to make use of the fact that people usually follow each other's behavior in situations of uncertainty (Klumpe et al., 2018). Moreover, websites use social proof to reduce concerns of users and therefore implement social proof nudges to build up trustworthiness (Schneider et al., 2019).

A study about the role of social proof and reciprocity in affecting user registrations by Roethke et al. (2020) used a social proof nudge in a registration layer on a website where participants were informed that 1 million user accounts had already been registered. Their study showed that the social proof nudge had a positive effect on users' registration.

A previous study about privacy nudges for mobile applications by Zhang and Xy (2016) found that social proof nudges reduce people's privacy concerns. In their study, the social proof nudge includes the percentage of other app users that approve the use of any type of data permissions. This serves as social norm indicator, reducing users' privacy concerns as other people do the same. Participants in this study felt comfortable to let the app use their personal information when they were presented with a social proof nudge. In addition, Acquisti et al. (2012) results showed that participants who were told that other participants disclosed private data, were more likely to reveal private data than participants who were not informed about other participant's revelations.

Based on these insights, it is expected that when people are presented with the social proof nudge, people will show less online privacy protection behavior than if they are not presented with the social proof nudge. Therefore, the first hypothesis is proposed:

***H_1*:** The presence of a social proof nudge is more negatively related to online privacy protection behavior compared to the absence of a social proof nudge.

Reciprocity nudge

According to Cialdini (2009), the norm of reciprocity requires people to respond to positive or negative actions with similar actions, thereby repaying the original actions. Moreover, reciprocity is the rule that obligates people to repay others for what they have received from them. According to Whatley et al. (1999) people have to deal with reciprocity at a young age to learn social cohesion and mutual benefit. In social exchanges, reciprocity plays a central role as it creates trust and helps to stabilize social relationships (Molm et al., 2007).

Reciprocity is often seen in the participation in a questionnaire to convince people to complete it. For example, Berry and Kanouse (1987) found that participants were more likely to complete a questionnaire when they received a gift, triggering their need to reciprocate, as opposed to when they were promised a gift after completing the questionnaire. In addition, the study by Roethke et al. (2020) used a reciprocity nudge in a welcome message on a website where participants were presented with a 5% discount voucher code. Their study showed that the reciprocity nudge had a positive effect on users' registration behavior.

A study by Acquisti et al. (2013) examining people's trade-offs between money and privacy shows that people attribute different values to their privacy protection. This study carried out two experiments in which people were asked to make a choice between gift cards that varied with respect to their privacy and monetary value. Their results showed that the minimum price people were willing to accept to disclose their data was higher than the maximum price they were willing to pay to prevent their data from being disclosed. Therefore, monetary gifts can effectively trigger reciprocity which reduces people's online privacy protection behavior by disclosing their personal data.

Based on these insights, it is expected that when people are presented with the reciprocity nudge, people will show less online privacy protection behavior than if they are not presented with the reciprocity nudge. Therefore, the second hypothesis is proposed:

H_2: The presence of a reciprocity nudge is more negatively related to online privacy protection behavior compared to the absence of a reciprocity nudge.

More or less nudging?

The first two hypotheses mentioned above have been formulated for the main effects of the social proof nudge and the reciprocity nudge on online privacy protection behavior. However, it raises the following question; "do the social proof nudge and reciprocity nudge interact with each other?". As stated in Chapter 2.2, there is a risk that a person will find it aggressive when he or she is being persuaded too coercively and therefore not appreciate it, resulting in reactance (Psychology Today, 2018). Based on this previous finding, it is expected in this study that when a person is persuaded too coercively by the means of both the social proof nudge and reciprocity nudge, the effect of the nudges disappears.

In addition, according to Jäger and Eisend (2013), when people recognize attempts of persuasion, they can evoke reactance. Attempts of persuasion can be seen as attempts to manipulate people's thoughts and actions in order to elicit the desired behavior. The desire for people to resist this manipulation and regain their freedom of choice triggers reactance, which is known as the theory of psychological reactance (Jäger & Eisend, 2013; Brehm, 1966). Reactance is a boomerang effect where the perception of coercion is answered with an equal but opposite influence that people use to restore their freedom of choice (Clee & Wicklund, 1980). The theory of psychological reactance by Brehm (1966) also points out circumstances in which persuasive actions may boomerang. This boomerang effect explains that, under certain circumstances, a persuasive action can cause changes in people's

behavior or attitude that deviate from the intended effect (Mann & Hill, 1984). In this study, it is expected that nudges will reduce people's online privacy protection behavior. However, when people are being persuaded too coercively by the means of two nudges, they might recognize this persuasive attempt and feel that their freedom of choice is being threatened resulting in reactance. Therefore, people can show a boomerang that deviates from the desired behavior.

These findings show that less nudging is better than more nudging. Moreover, based on these insights, it is hypothesized that when people are presented with both nudges, the effect of the nudge on online privacy protection behavior disappears:

H_{3a}: The effect of the reciprocity nudge on online privacy protection behavior disappears in the presence of the social proof nudge.

H_{3b}: The effect of the social proof nudge on online privacy protection behavior disappears in the presence of the reciprocity nudge.

2.3. Familiarity, uncertainty and quick decision

People are faced with uncertainty, time pressure and incomplete knowledge in their daily lives these days. Therefore, in these circumstances, people rely on simple heuristics which simplify their decision (Raue & Scholl, 2018). Moreover, according to Jung and Kellaris (2004), there are three boundary conditions within which nudges work; familiarity, uncertainty and quick decision. These conditions weaken or enhance the effect of the nudge on, in this study, online privacy protection behavior. Despite the large volume of scholarship on familiarity, uncertainty and quick decision by scientists, these terms are often not explicitly defined or otherwise defined in different (inconsistent) ways. More information about the three boundary conditions and their definitions in this study are being presented in the chapters below.

2.3.1. Familiarity

According to Jung and Kellaris (2004), decision heuristics, such as nudging according to Cialdini's principles, are more useful and likely to be applied when evaluative information is not available. When people cannot address evaluative information, there is a lack of familiarity. Lack of information is something that is often seen in the domain of privacy; the data holder has more information than the user. For example, when subscribing to a mail list, people do not know whether the mail list might be sold by the data holder to another party that could send spam mails (Acquisti et al., 2017). According to Park and Lessig (1981), familiarity is the level of how much a person knows about the object or the level of how much a person thinks he/she knows about the object. Familiarity is an understanding that is often based on previous interactions, experiences and learning from what, why, where and when others do what they do (Luhmann, 2017). In the present study, familiarity is defined as the level of knowledge about the corona-app and its online privacy aspects. According to Raue and Scholl (2018), when there is a lack of familiarity with an object, people use heuristics as shortcuts in decision making and nudges respond to a lack of knowledge. Based on this literature it can be assumed that when a person is more familiar with the corona-app and its privacy aspects, the person is less likely to rely on heuristics and therefore less prone to the nudge effect. Regardless of the type of nudge, it is hypothesized that the negative relationship between the nudge and online privacy protection behavior will be weaker when there is a high level of familiarity with the corona-app than when there is a low level of familiarity with the corona-app:

H_{4a}: The negative relationship between the reciprocity nudge and online privacy protection behavior will be weaker when there is a high level of familiarity with the app than when there is a low level of familiarity with the corona-app.

H_{4b}: : The negative relationship between the social proof nudge and online privacy protection behavior will be weaker when there is a high level of familiarity with the app than when there is a low level of familiarity with the corona-app.

2.3.2. Uncertainty

Nudges are more useful and likely to be applied when people want to minimize the uncertainty of the decision (Jung & Kellaris, 2004). Hofstede (1991) states the extent to which people feel threatened by uncertainty or unknown situations is known as uncertainty avoidance. Uncertainty avoidance is defined on an individual level as the degree to which an individual tries to avoid uncertainty as much as possible. According to Bar-Anan et al. (2009), uncertainty is defined as a lack of information about an object and has been characterized as an aversive state that people are motivated to reduce. In addition, uncertainty is the need for predictability to reduce this feeling. This predictability refers to the need for (un)written rules (Hofstede, 1991). In the present study, uncertainty is defined as the level of feeling uncertain about using the corona-app with its privacy aspects. In today's world, people have to make decisions under uncertain circumstances. In order to make a decision despite uncertainty, people rely on heuristics like a nudge in this case (Raue & Scholl, 2018). A study by Franklin et al. (2019) examined a series of choices under uncertain circumstances using nudge interventions. The obtained results of 1,423 participants showed that nudges strengthen their value as insights of choices under uncertain circumstances. In other words, when people are uncertain, the nudges have a higher value. Based on these findings, regardless of the type of nudge, it is hypothesized that the negative relationship between the nudge and online privacy protection behavior will be stronger when there is a high level of uncertainty regarding the corona-app than when there is a low level of uncertainty regarding the corona-app:

H_{5a}: The negative relationship between the reciprocity nudge and online privacy protection behavior will be stronger when there is a high level of uncertainty regarding the app than when there is a low level of uncertainty regarding the corona-app.

H_{5b}: The negative relationship between the social proof nudge and online privacy protection behavior will be stronger when there is a high level of uncertainty regarding the app than when there is a low level of uncertainty regarding the corona-app.

2.3.3. Quick decision

Nudges are more useful and likely to be applied when people are motivated to come to a quick decision, which can be circumstantial such as time pressure or internal (Jung & Kellaris, 2004). In the present study, quick decision is defined as the level of making a decision about using the corona-app in a limited time. As mentioned in Chapter 2.2, nudges would be most effective when they are applied to behavioral situations that are dominated by cognitive processes such as making choices under tight time constraints (Michalek et al., 2016). In addition, there is evidence that there is a relationship between people's decision making process and stressful situations, such as a situation where people experience a feeling of time pressure, as with quick decision making. Stress affects people's decision making by disrupting the scanning process and reducing their consideration of alternative

results (Cohen et al., 2012). When there is time pressure, which occurs in quick decision making, it can lead to a psychological conflict; time needed to perform a task is greater than the time available (Liu et al., 2017). People can only process a limited amount of information at a time. Therefore, people need to simplify their decision making. Heuristics have the advantage of reducing time and therefore they can help to make a choice. The presence of a nudge can be used as a heuristic, so it can be assumed that people who have to make a quick decision under time pressure, they will rely on the nudges when performing online privacy protection behavior. Based on this finding, regardless of the type of nudge, it is hypothesized that the negative relationship between the nudge and online privacy protection behavior will be stronger when there is a high level of quick decision regarding the corona-app than when there is a low level of quick decision regarding the corona-app:

H_{6a}: The negative relationship between the reciprocity nudge and online privacy protection behavior will be stronger when there is a high level of quick decision regarding the app than when there is a low level of quick decision regarding the corona-app.

H_{6b}: The negative relationship between the social proof nudge and online privacy protection behavior will be stronger when there is a high level of quick decision regarding the app than when there is a low level of quick decision regarding the corona-app.

2.4. Generational differences

Mannheim (1970) described a generational group, also known as a cohort, as a collective group of people born and raised in a similar location and who share historical and social life experiences. According to this description, people from different generations share experiences that influence their behavior and thoughts. Compared to older generations, Generation X and Generation Y were born before the popularization of the internet and are characterized by higher rates of internet adoption. This is due to the rapid adoption of internet use among the younger populations and their impressive purchase power (Lissitsa & Kol, 2016). The expectation is that online nudges will be mostly noticed by these two generations because of their characterization of high rates of internet adoption.

Generation X and Generation Y came from a different background and therefore have different coping skills and expectations (Reisenwitz & Lyer, 2009) (described in Chapters 2.4.1, 2.4.2 and 2.4.3). Research on generational differences has grown over the years. However, there is a lack of empirical research to validate the significance of generational differences (Salahuddin, 2010). Because there are multiple studies on generational differences, this study will describe Generation X and Generation Y based on 16 other studies that have more than 30 citations and have been published over the last 18 years.

Moreover, according to Smola and Sutton (2002), the labels of generations may be generally agreed upon, however the actual start and end dates used to define each generation, vary widely (see Table 1). This lack of consistency has implications for the definition of the generations and the assessment of their impact on outcomes. This study uses a time slot of 10 years for Generation X and Generation Y, leaving a 10-year difference between these generations. Therefore, Generation X consists of people who are born between 1965 and 1975. In addition, Generation Y consists of people who are born between 1985 and 1995.

Table 1
Definitions of the start and end dates of generations

According to	**Generation X**	**Generation Y**
Dainton & Zelley (2014)	People who are born between 1965 and 1980	People who are born between 1980 and 2000
Gurău (2012)	People who are born between 1961 and 1979	People who are born between 1980 and 1999
Smola & Sutton (2002)	People who are born between 1960 and 1982	People who are born between 1979 and 1994
Reisenwitz & Lyer (2009)	People who are born between 1965 and 1976	People who are born between 1977 and 1988
This study	People who are born between 1965 and 1975	People who are born between 1985 and 1995

2.4.1. Generations and online privacy protection behavior

Ruigrok NetPanel (2019), a Dutch market research agency, conducted a quantitative study in which they questioned the Dutch society about their internet use. This study has shown that in the Netherlands in 2019, Generation X and Generation Y show online privacy protection behavior because both generations have concerns about their online privacy.

For internet privacy in general, 43.9% of Generation Y is concerned about their privacy. When it comes to the privacy of their personal information, this generation is more often concerned with protecting the security of their personal information on the internet. Of all generations, Generation Y is most concerned with the privacy of personal data. 61% of this generation is concerned that their personal information will be misused. People from Generation Y change the privacy settings of social media so that their personal information does not end up 'on the street'.

After Generation X, Generation Y is most concerned with their privacy of personal data. 58% of this generation is concerned that their personal information will be misused. Generation X is aware of the dangers of internet use. Despite the awareness of online dangers, this generation less often adjusts the privacy settings of social media compared to Generation Y. People from this generation are sometimes unaware that they can influence the degree of privacy practice by changing privacy settings. Despite the fact that this generation does not adjust their privacy settings, this generation shows online privacy protection behavior by addressing the possible privacy concerns. When it comes to privacy in general, 45.5% of Generation X is concerned about their privacy.

Based on the characteristics of these two generations, it is expected that Generation X and Generation Y show online privacy protection behavior and therefore, the following hypotheses are proposed:

H_7: Generation X is positively related to online privacy protection behavior.
H_8: Generation Y is positively related to online privacy protection behavior.

2.4.2. Generation X and the social proof nudge

People from Generation X grew up with insecurity related to finance, family, social life, and experienced rapid change and great diversity, leading to individualism over collectivism (Smola & Sutton, 2002). Therefore, this generation is more skeptical, independent and less loyal compared to other generations (Glass, 2007).

According to Reisenwitz and Lyer (2009), Generation X is technologically savvy and will use it to personalize and humanize everything. In addition, Generation X has an attitude of risk avoidance and a low capacity for risk. This generation has certain levels of distrust, skepticism and has a self-sufficient attitude. Moreover, Generation X seeks customer convenience and community relations. This generation ignores advertising targeted to them and rejects any form of segmentation and marketing techniques. Although the generation is labeled as independent, individualistic, and self-sufficient, they do care about people's opinions, especially in times of uncertainty. This generation can be insecure about themselves and often needs reassurance that their choices are good (Wai Kwan Leung & Taylor, 2002). In addition, Generation X likes to research while shopping online more than other generations do. Therefore, this generation reads more reviews and visits more opinion sites compared to other generations (Parelta, 2015). Moreover, KPMG (2017) researched the behaviors and attitudes of Baby Boomers, Generation X and Generation Y towards online shopping. This research was conducted based on 18,430 customers living in more than 50 countries. This research revealed that 56% of Generation X researches online for reviews and recommendations before they make a purchase. Therefore, this generation relies on social cues from others to make purchase decisions. In addition, 49% of this generation shared feedback on the seller's website, which indicates that this generation finds it important to share feedback to help others make a choice.

Based on these findings and the characteristics of Generation X, it is expected that this generation will be sensitive to social proof nudges and therefore will show less online privacy protection behavior. Therefore, the following hypothesis is proposed:

H_9: The negative relationship between the social proof nudge and online privacy protection behavior will be stronger for Generation X than for Generation Y.

2.4.3. Generation Y and the reciprocity nudge

According to Howe and Strauss (2009), Generation Y can be described as team-oriented, achieving, pressured to do well, special, conventional, confident and sheltered. Moreover, Generation Y grew up in economic growth and technological developments, in particular the arrival of internet. Digital technologies are mediators of their lives and daily activities, and they have never known the way of life without digital technologies (Palfrey & gasser, 2013).

Generation Y is used to taking decisions faster and with less deliberation than Generation X and it is faster at adopting new opportunities (Parment, 2013). According to Reisenwitz and Lyer (2009), Generation Y is technology savvy and is more comfortable with technology compared to previous generations. In addition, according to the book of Twenge about Generation Me that was published in 2014, Generation Y is very extrinsic and materialistic, emphasizing money and image. Because of the great prosperity that Generation Y knows, this generation has its own problems; 'what does life bring me?' 'What is my added value for this life?' (Verhiel, 2017). Generation Y is constantly looking for the deal and wants to know what it will bring them. This generation wants to gain meaningful experiences and often asks 'what is in it for me?' if they see no result that benefits them (Papp & Matulich, 2011). According to the truth about online consumers 2017 Global Online Consumer Report by KPMG (2017), Generation Y wants to be treated as unique individuals

and is more impressed with offers from companies that have a personal element; 17% of this generation is driven by companies that anticipate needs based on customer profile and 29% of Generation Y prefers customized promotions. This indicates that the customer loyalty of Generation Y is driven by getting valued personal attributes. Moreover, compared to other generations, Generation Y more often choses an online supplier based on the price the website prefers (27%). This assumes that Generation Y wants to pay the best price for a product online and bases its choice for an online supplier on this.

Based on these findings and the characteristics of Generation Y, it is expected that this generation will be sensitive to reciprocity nudges and therefore will show less online privacy protection behavior. Therefore, the following hypothesis is proposed:

H_{10}: The negative relationship between the reciprocity nudge and online privacy protection behavior will be stronger for Generation Y than for Generation X.

2.4. Conceptual framework

As shown in Figure 3, the conceptual framework of this study includes eight variables. The social proof nudge and reciprocity nudge are independent variables and online privacy protection behavior is a dependent variable. Generation Y and Generation X are moderator variables. Moreover, familiarity, uncertainty and quick decision are moderator variables. These moderators are third variables which may affect the correlation between the social proof and reciprocity nudge, and the online privacy protection behavior.

In order to find out whether or not the online nudges influence Generation X and Generation Y in their online privacy protection behavior, the following research question is proposed: *"To what extent can social proof and reciprocity nudges influence the online privacy protection behavior of Generation X and Generation Y?".*

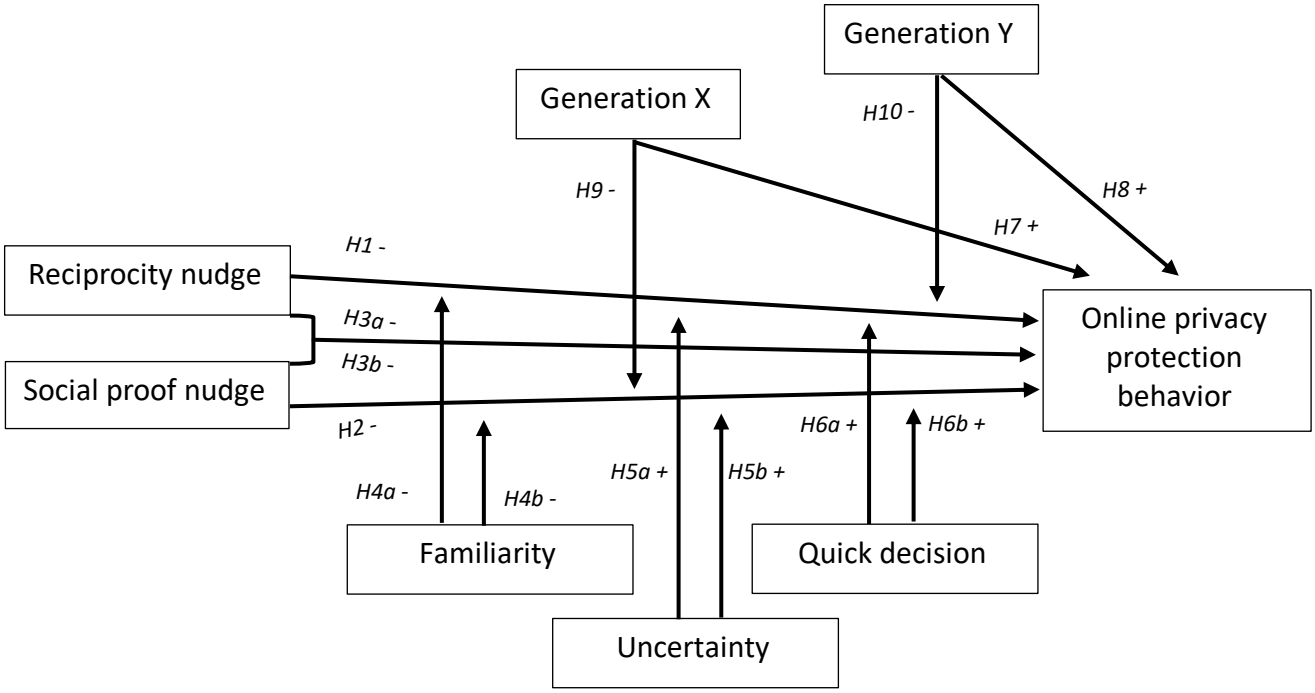

Figure 3. Conceptual framework

3. Study design and methodology

The study design and methodology section describes the study design, preliminary test, procedure, manipulations, instruments, data analysis and participants of the study.

3.1. Study design

The study consisted of a 2x2 between-subjects experimental design: there were two groups of social proof nudges (yes/no) and two groups of reciprocity nudges (yes/no). The dependent variable of this study was the online privacy protection behavior. The independent variables were the social proof nudge and reciprocity nudge. Different combination have been made between the social proof nudge and reciprocity nudge. Table 2 shows the four conditions of the study design and refers to the appendix which visualizes the conditions. This study has been approved by the ethical committee of the University of Twente.

Table 2
Study design

Condition	**Social proof nudge**	**Reciprocity nudge**	**Appendix**
Condition 1	Social proof nudge √	Reciprocity nudge √	Appendix 1
Condition 2	Social proof nudge √	Reciprocity nudge X	Appendix 2
Condition 3	Social proof nudge X	Reciprocity nudge √	Appendix 3
Condition 4	Social proof nudge X	Reciprocity nudge X	Appendix 4

Participants had to meet a number of requirements in order to participate in the study. The experiment took place in July 2020, after the first wave of the corona virus in the Netherlands. At the time of writing this study, the densely populated provinces of the Netherlands were hit harder by the corona virus compared to the sparsely provinces. People from densely populated provinces will therefore have a different view of the corona-app than people from sparsely populated provinces. Therefore, people living in the sparsely populated provinces of the Netherlands (Groningen, Friesland, Drenthe, Gelderland, Zeeland, Flevoland and Overijssel) took part in the study. In addition, the optimal goal was to have an equal number of people from Generation X and Generation Y for the study. Finally, all participants had to have experience with the internet.

3.2. Preliminary test

Before the experiment, a preliminary test was conducted by means of an (online) interview with a sample of eleven people in total; five people from Generation Y and six people from Generation X of which one person was a cybersecurity expert. This preliminary test indicated which wording of the social proof nudge and reciprocity nudge could best be used in the experiment. Further, this preliminary test prevented possible errors that may have appeared in the experiment, such as participants overlooking the nudge. The results of the preliminary test are shown in Appendix 6. In addition, the three items for the constructs of familiarity, uncertainty and quick decisions were based on items from previously tested studies but were shaped into the corona-app context. These created items were examined by two independent judges during a preliminary research. During this preliminary research, these judges were asked to evaluate whether each item represented the construct it was supposed to reflect, and whether each construct was represented by the items associated with it. These judges were also asked to evaluate whether each item was formulated clearly.

3.3. Procedure

Participants in the experiment were being asked to complete a questionnaire in 'Qualtrics' (see Appendix 7). The conditions were randomly assigned to participants in the experiment. The questionnaire was set up in such a way that participants had to answer all questions before continuing with the experiment. Moreover, the online questionnaire has been distributed on various online channels: Facebook, LinkedIn and Instagram. This method of data collection uses voluntary response sampling. Participants volunteered themselves by responding to the public online survey. In addition, several people shared the questionnaire through these online channels in their own network, resulting in a wide reach. This method of data collection uses snowball sampling where new participants are being recruited via existing participants. After the experiment, the outcomes were processed in SPSS. With SPSS, significant differences and conclusions were drawn.

3.4. Experimental manipulations

While conducting this study, the coronavirus broke out in the Netherlands and other parts of the world. The corona-app (CoronaMelder) is currently in development to prevent the spread of this virus by explaining whether or not a person has been in contact with someone who is infected with the virus (Consumentenbond, 2020). However, the downside of the corona-app is that it has a lot of privacy aspects. There is a risk that data will be used in a different way than intended and there is a risk that people's personal data will fall into the wrong hands (Autoriteit persoonsgegevens, 2020). Ministerie van Algemene Zaken (2020), or in English the Dutch Ministry of General Affairs, wants 60% of Dutch to participate in the corona-app and wants to do everything possible to stimulate participation as much as possible.

As can be concluded from the literature review (see Chapter 2.3), people who experience unfamiliarity, quick decision, uncertainty with an object will rely on a nudge to determine their online privacy protection behavior. The corona-app is used in this study because it was expected that it meets the three boundary conditions that enhance the nudge effect on online privacy protection behavior. First, the app does not yet exist in the Netherlands, that is why people are *unfamiliar* with the app and this will strengthen the effect of the two nudges on online privacy protection behavior. Secondly, there is much unclear about the corona-app and there have been many personal data leaks from previous versions of the app which increases people's feeling of *uncertainty* and this will strengthen the effect of the two nudges on online privacy protection behavior. Thirdly, the corona-app must be accepted quickly to maximize the effect of the app by preventing the spread of the coronavirus. This requires a *quick decision* from people to participate with the app, which will strengthen the effect of the two nudges on online privacy protection behavior. In the experiment, participants were asked to what extend they were familiar, uncertain and were willing to make a quick decision regarding the corona-app (see Table 4 for the exact statements).

For this study, the online privacy protection behavior in the fictional corona-app was manipulated with the social proof nudge and the reciprocity nudge. The condition with the social proof nudge was supposed to trigger a reduction in the online privacy protection behavior of Generation X in the fictional corona-app by presenting a social proof nudge. Figure 4 shows a possible formulation in Dutch of the social proof nudge, which is based on the premise that people would use the corona-app if they knew that others were also using the app. The English translation of the social proof nudge used in the privacy notification is "did you know that 42% of the Dutch already use this app?". The exact formulation of the social proof nudge for the study is conducted based on a preliminary test (see Appendix 5). The condition with the reciprocity nudge was supposed to trigger a reduction in the online

privacy protection behavior of Generation Y in the fictional corona-app by presenting a reciprocity nudge. Figure 5 shows an possible wording in Dutch of the reciprocity nudge, which is based on the premise that people would use the corona-app if they get something in return. The English translation of the reciprocity nudge used in the privacy notification is “did you know that by using this app you can see which places you can safely enter?”. The exact wording of the reciprocity nudge for the study is conducted based on a preliminary test (see Appendix 5).

Figure 4. Social proof nudge

Figure 5. Reciprocity nudge

3.5. Instruments

In this section, the instruments used in this study are further explained. Therefore, the questionnaire and the measures of variables are discussed.

3.5.1. The questionnaire

The questionnaire started with a short introduction to the content of the questionnaire and approval was requested for taking the questionnaire. Approval was required to participate in the questionnaire. The questionnaire consisted of four parts. In the first part demographic questions were asked. In the second part, questions were asked about the knowledge and opinion about the Dutch corona-app in development (CoronaMelder). In the third part, the participants were assigned to one of the four conditions. In this part, participants were being asked about a fictional interface of the corona-app while they were presented with a social proof nudge or not, were presented with a reciprocity nudge or not, were presented with both the social proof nudge and reciprocity nudge, and they were not presented with any nudge, based on the condition they were in (see Table 2). In the fourth part, the participants were asked about their online privacy protection behavior on the internet in general. After completing the fourth part,

participants were asked to confirm or withdraw their initial consent, because after this part they were informed that they may have been presented with a nudge. This information was withheld from the introduction of the questionnaire, because otherwise participants would be aware of the nudge and it could change their behavior and response to questions.

3.5.2. Measures

Social proof nudge and reciprocity nudge. In the experiment, conditions were randomly assigned to participants. In these conditions, participants were presented with a social proof nudge or not, were presented with a reciprocity nudge or not, were presented with both the social proof nudge and reciprocity nudge, or were not presented with any nudge. The social proof nudge and reciprocity nudge were measured by categorizing these variables into absent and present.

Generation X and Generation Y. These generations were measured by asking participants; "to which of the following two age categories do you belong?". The following two multiple choice answers were given "1965 – 1975" or "1985-1995". If participants chose for 1965 – 1975, they were measured as Generation X and if they chose for 1985-1995, they were measured as Generation Y.

Online privacy protection behavior. The online privacy protection behavior was measured with items that assess three coping strategies: fabricate, search, and refrain. Each coping strategy was rated with two items. Skills were used from a prior study about people's privacy protection behavior by Youn (2009) to create items for online privacy protection behavior. In their study, many other privacy-related studies were used as input for the items. In this study, online privacy protection behavior of participants was measured in two different ways: the online privacy protection behavior in general on the internet and the online privacy protection behavior in the fictional corona-app. Participants were asked to what extent they agreed with the statements based on a 5-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = not disagree/not agree; 4 = agree and 5 = strongly agree). Table 4 shows the exact items of online privacy protection behavior on the internet and in the fictional corona-app. For the two constructs, six items were combined to get a measurable overall variable of online privacy protection behavior in the fictional corona-app (M = 2.78*,* SD = .75) and a measurable overall variable of online privacy protection behavior on the internet (M = 2.61*,* SD = .71). The Cronbach's alpha in Table 4 was calculated to confirm internal consistency of the constructs. A Cronbach's alpha of .70 and above is considered acceptable (Multon & Coleman, 2012). Sufficient internal consistency is confirmed for the construct of online privacy protection behavior on the internet (α = .72). In addition, the Cronbach's alpha of the construct of online privacy protection behavior in the fictional corona-app is very close to the acceptable limit of .70. (α = .68). Deleting item(s) from this construct would not improve the Cronbach's alpha. In addition, as a large number of items may artificially inflate the Cronbach's alpha, a smaller set of items may artificially deflate the Cronbach's alpha (Multon & Coleman, 2012). Therefore, for a scale of only six items, an Cronbach's alpha of .68 is considered acceptable. Furthermore, online privacy protection behavior contains construct validity because the constructs were based on items from previously tested studies.

***Familiarity, uncertainty and quick decision*.** Familiarity, uncertainty and quick decision regarding the actual corona-app in development (CoronaMelder) were each measured with three created items. Familiarity was measured by creating three items that reflected important aspects of familiarity with the corona-app and its privacy aspects. These items were based on familiarity items of a previous study by Gefen (2000). In addition, uncertainty was measured with three created items that reflected aspects of uncertainty

people had regarding the corona-app and its privacy aspects. These items were based on a previous study by Jung and Kellaris (2004) who based their items on Hofstede's definition of uncertainty avoidance (Hofstede, 1991). Furthermore, quick decision was measured with three created items that reflected the aspects of quick decision with the corona-app. These items were based on the importance of using the corona-app within a short timeframe (Ministerie van Algemene Zaken, 2020). The set of items for familiarity, uncertainty and quick decision were assessed on a 5-point Likert scale (1 = strongly disagree; 2 = disagree; 3 = not disagree/not agree; 4 = agree and 5 = strongly agree). Table 4 shows the exact items of familiarity, uncertainty and quick decision. For each construct, three items were combined to obtain a measurable overall variable of familiarity (*M* = 2.50*, SD* = .96), a measurable overall variable of uncertainty (*M* = 2.99*, SD* = .97) and a measurable overall variable of quick decision (*M* = 3.38*, SD* = .96). Furthermore, as shown in Table 4, sufficient internal consistency is confirmed since the constructs familiarity (α = .89), uncertainty (α = .78) and quick decision (α = .86) are all above .70. In addition, these items were created based on items from previously tested studies and then examined by independent judges who did not participate in the item creating session (see Chapter 3.2). These judges evaluated whether each item represents the construct it should reflect, and whether each construct was represented by the created items. Therefore, there is content validity.

Table 4
Internal consistency

Construct		Items	α
Online privacy protection behavior fictional corona-app	1.	Seeing this image, I give up a made-up name or identity in the following step of the app where I have to enter my personal data.	.68
	2.	Seeing this image, I provide incomplete information about myself in the next step of the app where I have to enter my personal data.	
	3.	Seeing this image, I ask someone (e.g. parents or friends) for advice before ticking all the boxes and clicking on "accept" and leave my personal data behind.	
	4.	Seeing this image, I first read the app's privacy statement before ticking all the boxes and clicking on "accept" and leave my personal data behind.	
	5.	Seeing this image, I will use a different app that does not ask for my personal data.	
	6.	Seeing this image, I leave the app and will not use it.	
Online privacy protection behavior internet	1.	If I have to fill in my personal data online, I give a made-up name or identity.	.72
	2.	If I have to fill in my personal data online, I provide incomplete information about myself.	
	3.	If I have to fill in my personal data online, I ask someone (e.g. parents or friends) for advice.	
	4.	If I have to fill in my personal data online, I first read the privacy statement of the website / app.	
	5.	If I need to fill in my personal data online, I will go to other websites / apps who do not ask for my personal data.	
	6.	If I have to fill in my personal data online, I leave the website / app and will not use it.	
Familiarity	1.	I am familiar with the corona-app and I know exactly what this app is.	.89
	2.	I am familiar with the privacy aspects of the corona-app and I know exactly which consequences this has for my privacy and freedom.	
	3.	I am familiar with the risks associated with the corona-app and I know exactly what consequences this has for my privacy.	
Uncertainty	1.	I feel uncertain about using the corona-app when I do not know which outcome this app offers.	.78
	2.	I am not at risk of my privacy data being used by the corona-app when the outcome of this app cannot be predicted.	
	3.	I feel stressed when I cannot predict the consequences of using the corona-app.	
Quick decision	1.	To limit the spread of the corona virus, I make a quick decision about whether or not to use the corona-app.	.86
	2.	60% of the Dutch must use the corona-app to replace all other corona measures and that is why I make a quick decision whether or not to use the corona-app.	
	3.	To find out if I have been in contact with persons infected with the coronavirus, I come to a quick decision whether or not to use the corona-app.	

Note: all the above items were asked in Dutch

3.6. Data analysis

To test whether there were differences between the four conditions regarding the characteristics of participants, a randomization check was performed, as will be presented in Table 3. A Person's Chi-square test was performed to analyze whether there were differences between the four conditions regarding the generation, gender, educational attainment and residence of participants. In addition, to analyze whether there were differences between the conditions regarding participants' internet experience, internet use and app use, a one-way ANOVA was used. Furthermore, a reliability analysis was conducted with Cronbach's alpha to check the internal consistency of the constructs.

The aim of this study is to examine the effect of the social proof nudge and reciprocity nudge on the online privacy protection behavior of Generation X and Generation Y. These effects were tested by performing GLM Univariate analysis (ANOVA). The social proof nudge and reciprocity nudge were both categorized as absent and present. Because the interaction between the nudge and the online privacy protection behavior was expected to be moderated by generation, familiarity, uncertainty and quick decision, a GLM Univariate analysis (ANOVA) was also performed for all these moderator variables. A median split was used to categorize familiarity (*Mdn* = 2.33), uncertainty (*Mdn* = 3.00) and quick decision (*Mdn* = 2.67) in a low and high level. Generation was categorized in Generation X and Generation Y. Furthermore, online privacy protection on the internet and online privacy protection behavior in the fictional corona-app between manipulations were analyzed using a one-way ANOVA. Moreover, a paired-sample t-test was performed to see whether there was a difference between the online privacy protection behavior on the internet and in the fictional corona-app. The one-way ANOVA was also used for analyzing the online privacy protection behavior on the internet and online privacy protection behavior between generations. Further, information sharing in the fictional corona-app was measured using the one-way ANOVA. Additional post-hoc tests (LSD and Bonferroni) were performed to see whether there was a specific group of data that differed from the three data groups

All data were analyzed by the statistical software program IBM SPSS Statistics 25. The percentages or means were reported with a confidence interval of 95%. In addition, the significance level of the *p*-value lower than .05 was used as a threshold for significant difference.

3.7. Participants

In this study, a total of 286 participants remained. However, 442 people started completing the online questionnaire. 142 people did not participate in the study because they did not approve with the terms, did not live in the correct provinces, did not fill in the questionnaire completely, or did withdraw their initial consent. In addition, 2 people who spent less than 3 minutes on the questionnaire were excluded from the study because they were outliers and it can be assumed that they did not look closely at the picture and questions to answer the questions correctly. Moreover, 12 people who spent more than 40 minutes on the questionnaire were excluded from the study because they were outliers. Moreover, given the long time it took them to complete the questionnaire, it can be assumed that the difficultly level of the questions was too high for these participants to answer the questions correctly.

Table 3 provides an overview of the characteristics of the participants in the study. In addition, the table contains a randomization check of the differences between the four conditions regarding the characteristics of participants. 286 participants took part in the experiment, of which 69 were in condition 1, 76 were in condition 2, 66 were in condition 3 and 75 participants were in condition 4. In this study, Generation X includes people who

were born during 1965-1975 and are in the 45-55 age range as of 2020. Moreover, Generation Y includes people who were born during 1985-1995 and are in the 25-35 age range as of 2020. A Pearson's Chi-square test was performed to analyze whether there were differences between the four conditions regarding the generation of the participants. This test showed that there was no significant difference, χ^2 (3) = 1.23 *p* = .747. However, Table 3 shows that in total more people from Generation X (*N* = 161) than Generation Y (*N* = 125) participated in the experiment. In addition, the Person's Chi-square test showed that there was no difference between the different conditions regarding participants' gender, χ^2 (3) = 2.81 *p* = .422. However, as Table 3 shows, overall more women (*N* = 184) than men (*N* = 102) took part in the experiment. Educational attainment is classified in 'low education' and 'high education'. Low education stands for preparatory secondary vocational education, general secondary education, pre-university education and secondary vocational education. High education stands for higher professional education, university bachelor degree, university master degree and PhD. In total, most participants had a high education attainment (*N* = 183). The Person's Chi-square test shows that there was no difference between the conditions regarding the educational level of participants, χ^2 (3) = 18.11 *p* = .642. Moreover, in the experiment, internet experience was measured with a 5-point Likert scale. In Table 3, internet experience is measured by the mean and standard deviation: *M(SD*). These statistics show that participants in all conditions had high internet experience. There were no significant differences between the conditions regarding internet experience as determined by the one-way ANOVA, *F*(3,282) = 0.75 *p* = .525. In addition, internet use was measured in the experiment by giving participants four options to choose from: 0 hours a day, 1 to 3 hours a day, 4 to 6 hours a day and more than 6 hours a day. Table 3 shows participant's average internet use in hours per day. Moreover, the one-way ANOVA shows that there was no difference between the conditions regarding the internet use of participants, *F*(3,282) = 0.45 *p* = .718. No participant indicated that he or she used the internet 0 hours a day. Therefore, it can be assumed that all participants had online experience. Furthermore, corona-app use was measured in the experiment with a 5-point Likert scale. For this construct, three items were combined to get a measurable overall variable of corona-app use (*M* = 2.75, *SD* = 1.04), sufficient internal consistency is confirmed (α = .93). In Table 3, corona-app use is measured by the mean and standard deviation: *M(SD)*. According to the one-way ANOVA test, there was no significance difference between the conditions regarding the corona-app use of participants, *F*(3,282) = 0.40 *p* = .754. Furthermore, Table 3 shows that most participants in all conditions lived in Overijssel (*N = 264*). In addition, the participants lived in Gelderland (*N = 14)*, Groningen (*N = 3)*, Drenthe (*N = 3)* and Friesland (*N = 2)*. None of the participants lived in Noord-Holland, Zuid-Holland, Noord-Brabant, Utrecht, Limburg, Zeeland and Flevoland. The Person's Chi-square test shows that there was a difference between the conditions regarding the residence of participants, χ^2 (12) =21.67 *p* = .041. Participants from Overijssel were equally divided over condition 1 (98.6%), 3 (93.9%) and 4 (92%). However, in proportion to these conditions, there were fewer participants from Overijssel in condition 2. In addition, there were no participants from Gelderland in condition 1, while these participants were in condition 2 (10.5%), 3 (1,5%) and 4 (6.7%). Further, there were no participants from Groningen in condition 1, while these participants were equally divided among the other conditions (1.3%). Moreover, there were no participants from Friesland in conditions 1,3 and 4, while these participants were in condition 2 (2.6%). Furthermore, there were no participants from Drenthe in conditions 2 and 4, while these participants were in conditions 1 (1.4%) and 3 (3%).

Table 3
Demographic characteristics

	Condition 1 (*N* = 69)	**Condition 2 (*N* = 76)**	**Condition 3 (*N* = 66)**	**Condition 4 (*N* = 75)**	**Total (*N* = 286)**	***p***
Generation						.747[a]
Generation X	42 (60.9%)	42 (55.3%	38 (57.6%)	39 (52%)	161 (56.3%)	
Generation Y	27 (39.1%)	34 (44.7%)	28 (42.4%)	36 (48%)	125 (43.7%)	
Gender						.422[a]
Men	30 (43.5%)	27 (35.5%)	22 (33.3%)	23 (30.7%)	102 (35.7%)	
Women	39 (56.5%)	49 (64.5%)	44 (66.7%)	52 (69.3%)	184 (64.3%)	
Educational attainment						.642[a]
Low	23 (33.3%)	30 (39.4%)	19 (28.7%)	31 (41.3%)	103 (36%)	
High	46 (66.7%)	46 (60.6%)	47 (71.3%)	44 (58.7%)	183 (64%)	
Internet experience scale of 1 to 5	4.25 (.85)	4.21 (.85)	4.11 (.86)	4.05 (.96)	4.15 (.88)	.525[b]
Internet use hours per day	3 (2)	3 (2)	4 (2)	4 (2)	4 (2)	.718 [b]
Corona-app use scale of 1 to 5	2.66 (1.10)	2.72 (1.10)	2.75 (.99)	2.84 (.99)	2.75 (1.04)	.754[b]
Recidence						.041[a]
Overijssel	68 (98.6%)	65 (85.5%)	62 (93.9%)	69 (92%)	264 (92.3%)	
Gelderland	-	8 (10.5%)	1 (1.5%)	5 (6.7%)	14 (5%)	
Groningen	-	1 (1.3%)	1 (1.3%)	1 (1.3%)	3 (1%)	
Friesland	-	2 (2.6%)	-	-	2 (0.7%)	
Drenthe	1 (1.4%)	-	2 (3%)	-	3 (1%)	
Other	-	-	-	-	-	

[a] *p* values calculated by Chi-square test
[b] *p* values calculated by ANOVA test

4. Results

In the results section, the outcomes of the experiment are analyzed. The first paragraph focuses on the main effects of the social proof nudge and reciprocity nudge on online privacy protection behavior. In addition, the moderation of the social proof nudge and reciprocity nudge on online privacy protection behavior are being addressed. The second paragraph focuses on the online privacy protection behavior between manipulations and the online privacy protection behavior between generations. Moreover, to found out more about the online privacy protection behavior in the fictional corona-app, the extent to which participants share information in the app is being analyzed.

4.1. The main effect of the nudges

The main effects of the independent variables were measured using a GLM Univariate analysis (ANOVA). The ANOVA was performed with the following independent variables: social proof nudge (absent vs. present) and reciprocity nudge (absent vs. present). In addition, online privacy protection behavior in the fictional corona-app was included as dependent variable. After measuring the main effects of the independent variables, the interaction effects between these variables were measured. This analysis is also used in Chapter 4.1.1, but in combination with a different moderator variable as an independent variable each time.

As Table 5 shows, of the 286 participants, 141 participants were not presented with a social proof nudge and 145 participants were presented with this nudge. Moreover, 151 participants were not presented with the reciprocity nudge and 135 participants were presented with this nudge. In addition, Table 5 shows the mean and standard deviation of online privacy protection behavior for the absence and presence of the social proof nudge and reciprocity nudge: *M(SD).*

The test showed that the main effect of the social proof nudge on online privacy protection behavior was not significant, $F(1,282) = 0.70$ $p = .404$. In addition, as presented in Table 5, there was no significant main effect of the reciprocity nudge on online privacy protection behavior, $F(1,282) = 0.16$ $p = .692$.

Furthermore, the interaction effect between the social proof nudge and reciprocity nudge did not turn out to be significant, $F(1,282) = 0.34$ $p = .561$.

Table 5
Effects of nudges on online privacy protection behavior corona-app

		M(SD)	*N*	Sum of Squares	*df*	*df error*	Mean Square	*F*	*p*
Social proof	Absent	2.74 (.71)	141	0.40	1	282	0.40	0.70	.404
	Present	2.81 (.79)	145						
Reciprocity	Absent	2.80 (.78)	151	0.09	1	282	0.09	0.16	.692
	Present	2.76 (.73)	135						
Social proof * Reciprocity				0.19	1	282	0.19	0.34	.561

4.1.1. The moderation of the effect of nudges

Generations

In addition to the descriptive statistics of the social proof nudge and reciprocity nudge, Table 6 shows that 161 participants were from Generation X and 125 participants were from Generation Y. Moreover, Table 6 shows the mean and standard deviation of online privacy protection behavior for the absence and presence of the nudges and for the generations: *M(SD).*

Furthermore, Table 6 shows that the main effect of the social proof nudge on participant's online privacy protection behavior was not significant, $F(1,278) = 0.84$ $p = .362$. In addition, the table shows that there was not a significant main effect of the reciprocity nudge, $F(1,278) = 0.41$ $p = .525$. Moreover, the main effect of generation on online privacy behavior turned out to be not significant, $F(1,278) = 1.97$ $p = .161$.

Further, there was no significant interaction effect between the social proof nudge and the reciprocity nudge, $F(1,278) = 0.51$ $p = .478$. In addition, the interaction effect between the social proof nudge and generation was not significant, $F(1,278) = 0.23$ $p = .630$. Moreover, no significant interaction effect was found between the reciprocity nudge and generation, $F(1,278) = 2.56$ $p = .111$.

Table 6
Effects of nudges and generations on online privacy protection behavior corona-app

		M(SD)	*N*	Sum of Squares	*df*	*df error*	Mean Square	*F*	*p*
Social proof	Absent	2.74 (.71)	141	0.47	1	278	0.47	0.84	.362
	Present	2.81 (.79)	145						
Reciprocity	Absent	2.80 (.78)	151	0.23	1	278	0.23	0.41	.525
	Present	2.76 (.73)	135						
Generation	Generation X	2.83 (.76)	161	1.11	1	278	1.11	1.97	.161
	Generation Y	2.71 (.73)	125						
Social proof * Reciprocity				0.29	1	278	0.29	0.51	.478
Social proof * Generation				0.13	1	278	0.13	0.23	.630
Reciprocity * Generation				1.45	1	278	1.45	2.56	.111

Familiarity

In addition to the descriptive statistics of the nudges and generations, Table 7 shows that 117 participants had low familiarity with the corona-app and 169 participants had high familiarity with the corona-app. The table shows the mean and standard deviation of online privacy protection behavior for the level of familiarity, for the absence and presence of the nudges and for the generations: *M(SD).*

In addition, Table 7 shows that the main effect of the social proof nudge on online privacy protection behavior was not significant, $F(1,270) = 0.74$ $p = .390$. Moreover, there was no significant main effect of the reciprocity nudge, $F(1,270) = 0.90$ $p = .343$. Further, there was no significant main effect of generation on online privacy protection behavior, $F(1,270) = 2.41$ $p = .122$. However, a significant main effect was found for familiarity on online privacy protection behavior, $F(1,270) = 4.65$ $p = .032$. As presented in Table 7, most people ($N = 169$) had a high familiarity with the corona-app and showed less online privacy protection behavior ($M = 2.70$, $SD = 0.74$) than people with low familiarity with the corona-app ($M = 2.90$, $SD = 0.75$).

Furthermore, the interaction effect between the social proof nudge and reciprocity was not significant, $F(1,270) = 0.27$ $p = .601$. In addition, no significant interaction effect was found between the social proof nudge and generation, $F(1,270) = 0.11$ $p = .740$. There was also no significant interaction effect between the social proof nudge and familiarity, $F(1,270) = 0.49$ $p = .486$. Moreover, the interaction effect between the reciprocity nudge and generation turned out to be not significant, $F(1,270) = 2.40$ $p = .123$. This also applies to the interaction effect between the reciprocity nudge and familiarity, $F(1,270) = 2.03$ $p = .155$. Finally, no significant interaction effect was found between familiarity and generation, $F(1,270) = 0.07$ $p = .791$.

Table 7
Effects of nudges, generations and familiarity on online privacy protection behavior corona-app

		M(SD)	*N*	Sum of Squares	*df*	*df error*	Mean Square	*F*	*p*
Social proof	Absent	2.74 (.71)	141	0.41	1	270	0.41	0.74	.390
	Present	2.81 (.79)	145						
Reciprocity	Absent	2.80 (.78)	151	0.50	1	270	0.50	0.90	.343
	Present	2.76 (.73)	135						
Generation	Generation X	2.83 (.76)	161	1.34	1	270	1.34	2.41	.122
	Generation Y	2.71 (.73)	125						
Familiarity	Low	2.90 (.75)	117	2.59	1	270	2.59	4.65	.032
	High	2.70 (.74)	169						
Social proof * Reciprocity				0.15	1	270	0.15	0.27	.601
Social proof * Generation				0.06	1	270	0.06	0.11	.740
Social proof * Familiarity				0.27	1	270	0.27	0.49	.486
Reciprocity * Generation				1.33	1	270	1.33	2.40	.123
Reciprocity * Familiarity				1.13	1	270	1.13	2.03	.155
Generation * Familiarity				0.04	1	270	0.04	0.07	.791

Uncertainty

In addition to the descriptive statistics of the nudges and generations, Table 8 shows that 124 participants had a low feeling of uncertainty about the corona-app and 162 participants had a high feeling of uncertainty about the corona-app. The table shows the mean and standard deviation of online privacy protection behavior for the level of uncertainty, for the absence and presence of the nudges and for the generations: *M(SD).*

In addition, Table 8 shows that the main effect of the social proof nudge on online privacy protection behavior was not significant, $F(1,270) = 0.35$ $p = .557$. Further, the main effect of the reciprocity nudge turned out to be not significant, $F(1,270) = 0.88$ $p = .349$. Moreover, there was no significant main effect for generation on online privacy protection behavior, $F(1,270) = 0.22$ $p = .643$. However, a significant main effect was found for uncertainty on online privacy protection behavior, $F(1,270) = 48.54$ $p = <.001$. As presented in Table 8, most people ($N = 162$) had a high feeling of uncertainty about the corona-app and showed more online privacy protection behavior ($M = 3.04$, $SD = 0.70$) than people with a low feeling of uncertainty about the corona-app ($M = 2.44$, $SD = 0.68$).

Furthermore, there was no significant interaction effect between the social proof nudge and reciprocity nudge, $F(1,270) = 0.36$ $p = .550$. Moreover, no significant interaction effect was found between the social proof nudge and generation, $F(1,270) = 0.16$ $p = .688$. There was also no significant interaction effect between the social proof nudge and uncertainty, $F(1,270) = 0.18$ $p = .671$. In addition, the interaction effect between the reciprocity nudge and generation turned out to be not significant, $F(1,270) = 4.10$ $p = .044$. This also applies to the interaction effect between the reciprocity nudge and uncertainty, $F(1,270) = 0.00$ $p = .997$. Finally, no significant interaction effect was found between uncertainty and generation, $F(1,270) = 0.06$ $p = .806$.

Table 8
Effects of nudges, generations and uncertainty on online privacy protection behavior corona-app

		M(SD)	*N*	Sum of Squares	*df*	*df error*	Mean Square	*F*	*p*
Social proof	Absent	2.74 (.71)	141	0.20	1	270	0.20	0.35	.557
	Present	2.81 (.79)	145						
Reciprocity	Absent	2.80 (.78)	151	0.43	1	270	0.43	0.88	.349
	Present	2.76 (.73)	135						
Generation	Generation X	2.83 (.76)	161	0.11	1	270	0.11	0.22	.643
	Generation Y	2.71 (.73)	125						
Uncertainty	Low	2.44 (.68)	124	23.74	1	270	23.74	48.54	.000
	High	3.04 (.70)	162						
Social proof * Reciprocity				0.18	1	270	0.18	0.36	.550
Social proof * Generation				0.08	1	270	0.08	0.16	.688
Social proof * Uncertainty				0.09	1	270	0.09	0.18	.671
Reciprocity * Generation				2.00	1	270	2.00	4.10	.044
Reciprocity * Uncertainty				7.00	1	270	7.00	0.00	.997
Generation * Uncertainty				0.03	1	270	0.03	0.06	.806

Quick decision

In addition to the descriptive statistics of the nudges and generations, Table 9 shows that 74 participants had a low level of quick decision about using the corona-app and 212 participants had a high level of quick decision about the corona-app. The table shows the mean and standard deviation of online privacy protection behavior for the level of quick decision, for the absence and presence of the nudges and for the generations: *M(SD).*

Furthermore, Table 9 shows that the main effect of the social proof nudge on online privacy protection behavior was not significant, $F(1,270) = 0.56$ $p = .453$. In addition, the main effect of the reciprocity nudge turned out to be not significant, $F(1,270) = 0.31$ $p = .580$. Moreover, there was no significant main effect for generation on online privacy protection behavior, $F(1,270) = 1.22$ $p = .271$. However, the main effect of quick decision on online privacy protection behavior was significant, $F(1,270) = 13.88$ $p = <.001$. Table 9 shows that most people ($N = 212$) had a high level of quick decision about using the corona-app and showed less online privacy protection behavior ($M = 2.67$, $SD = 0.74$) than people with a low level of quick decision about using the corona-app ($M = 3.08$, $SD = 0.72$).

Further, the interaction effect between the social proof nudge and reciprocity nudge was not significant, $F(1,270) = 0.51$ $p = .477$. Moreover, there was no significant interaction effect between the social proof nudge and generation, $F(1,270) = 0.01$ $p = .921$. There was also no significant interaction effect between the social proof nudge and quick decision, $F(1,270) = 0.04$ $p = .837$. In addition, the interaction effect between the reciprocity nudge and generation was not significant, $F(1,270) = 1.65$ $p = .200$. This also applies to the interaction effect between the reciprocity nudge and quick decision, $F(1,270) = 0.06$ $p = .805$. Finally, no significant interaction effect was found between quick decision and generation, $F(1,270) = 0.00$ $p = .993$.

Table 9
Effects of nudges, generation and quick decision on online privacy protection behavior corona-app

		M(SD)	*N*	Sum of Squares	*df*	*df error*	Mean Square	*F*	*p*
Social proof	Absent	2.74 (.71)	141	0.31	1	270	0.31	0.56	.453
	Present	2.81 (.79)	145						
Reciprocity	Absent	2.80 (.78)	151	0.17	1	270	0.17	0.31	.580
	Present	2.76 (.73)	135						
Generation	Generation X	2.83 (.76)	161	0.67	1	270	0.67	1.22	.271
	Generation Y	2.71 (.73)	125						
Quick decision	Low	3.08 (.72)	74	7.61	1	270	7.61	13.88	.000
	High	2.67 (.74)	212						
Social proof * Reciprocity				0.28	1	270	0.28	0.51	.477
Social proof * Generation				0.01	1	270	0.01	0.01	.921
Social proof * Quick decision				0.02	1	270	0.02	0.04	.837
Reciprocity * Generation				0.91	1	270	0.91	1.65	.200
Reciprocity * Quick decision				0.03	1	270	0.03	0.06	.805
Generation * Quick decision				4.61	1	270	4.61	0.00	.993

4.2. Online privacy protection behavior

Table 10 presents an overview of the four manipulations and the online privacy protection behavior of participants in general on the internet and in a fictional corona-app interface. These statistics were measured in the experiment with a 5-point Likert scale. The table shows the mean and standard deviation of online privacy protection behavior on the internet and in the fictional corona-app for the manipulations: *M(SD).* As the table shows, participants in all manipulations scored slightly higher than average on online privacy protection behavior on the internet, which means that all participants showed online privacy protection behavior on the internet. According to the ANOVA test, there was no significant difference between the four manipulations regarding online privacy protection behavior on the internet, $F(3,282) = 0.12$ $p = .949$.

Furthermore, Table 10 shows that participants in all manipulations scored higher than average on online privacy protection behavior in the fictional corona-app, which means that all participants showed online privacy protection behavior in the fictional corona-app, whether or not they were presented with a nudge. According to the ANOVA test, there was no significant difference found between the manipulations regarding online privacy protection behavior in the fictional corona-app, $F(3,282) = 0.38$ $p = .770$.

Table 10
Online privacy protection behavior and manipulations

	Online privacy protection behavior internet		Online privacy protection behavior corona-app	
Manipulation	*M*	*SD*	*M*	*SD*
Social proof and reciprocity	2.59	0.59	2.82	0.76
Social proof	2.65	0.82	2.81	0.82
Reciprocity	2.58	0.71	2.70	0.69
No manipulation	2.60	0.68	2.78	0.73
Total	2.61	0.71	2.78	0.75

In addition, a paired-sample t-test was performed to see if there was a difference between the online privacy protection behavior on the internet and in the fictional corona-app. According to this test, there was a significant difference in the scores for online privacy protection behavior internet (*M* = 2.61, *SD* = 0.71) and online privacy protection behavior corona-app (*M* = 2.78, *SD* = 0.75); t(285) = -5.37, *p* = <.001.

4.2.1. Generations and online privacy protection behavior

Table 11 presents an overview of the generations and their online privacy protection behavior on the internet and in a fictional corona-app interface. These statistics were measured in the experiment with a 5-point Likert scale. The table shows the mean and standard deviation of online privacy protection behavior on the internet and online privacy protection behavior in the fictional corona-app for the generations: *M(SD)*. According to the ANOVA test, there was a significant difference between the two generations regarding online privacy protection behavior on the internet, *F*(1,284) = 8.53 *p* = .004. The difference is that Generation X showed more online privacy protection behavior on the internet *(M* = 2.71, *SD* = 0.70) compared to Generation Y (*M* = 2.47, *SD* = 0.69).

Furthermore, Table 11 shows that the two generations scored higher than average on online privacy protection behavior in the fictional corona-app, which means that all participants showed online privacy protection behavior in the fictional corona-app, whether or not they were presented with a nudge. According to the ANOVA test, there was no significant difference found between two generations regarding online privacy protection behavior in the app, *F*(1,284) = 1.67 *p* = .198.

Table 11
Online privacy protection behavior and generations

	Online privacy protection behavior internet		Online privacy protection behavior corona-app	
Generation	*M*	*SD*	*M*	*SD*
Generation X	2.71	0.70	2.83	0.76
Generation Y	2.47	0.69	2.71	0.73

4.2.2. Information sharing in the app

To found out more about the online privacy protection behavior of participants in the fictional corona-app, the extent to which participants shared information in the app is being analyzed. Table 12 presents an overview of the four manipulations in combination with information sharing in terms of willingness to accept that the app would use three types of private data. This table shows the mean and standard deviation of health data, personal data, location data for the manipulations: *M(SD).* These statistics were measured in the experiment with a slider bar on a scale from 0 to 100. Value 0 means that a person was unwilling to accept that the app used these data and the value of 100 means that a person was willing to accept this. In general, the table shows that participants in all manipulations were most willing to accept that their location data was being used by the corona-app (*M* = 60.84, *SD* = 35.73). After that, participants in all manipulations were willing to accept that the app used their health data (*M* = 53.85, *SD* = 35.39). In addition, participants in all manipulations were the most unwilling to accept that their personal data was being used (*M* = 38.46, *SD* = 32.07). Frequently mentioned reasons for willing to accept that the app used these private data were “important”, “no problem”, “necessary” and “fight corona”. Frequently mentioned reasons for unwilling to accept this were “not their business”, “private”, “safety issues” and “distrust”. An ANOVA test was performed to compare the means and to find out whether there was a significant difference between the four manipulations. There was not found a significant difference between the manipulations regarding health data ($F(3,282) = 0.74$ $p = .531$), personal data ($F(3,282) = 0.80$ $p = .494$) and location data ($F(3,282) = 0.95$ $p = .417$).

Table 12
Information sharing and manipulations

	Health data		Personal data		Location data	
Manipulation	*M*	*SD*	*M*	*SD*	*M*	*SD*
Social proof and reciprocity	50.72	36.37	34.42	31.24	57.61	34.91
Social proof	56.91	34.78	38.49	33.03	62.83	36.63
Reciprocity	50.38	36.03	37.88	32.59	65.91	33.29
No manipulation	56.67	34.71	42.67	31.51	57.33	37.62
Total	53.85	35.39	38.46	32.07	60.84	35.73

In addition, post-hoc tests (LSD and Bonferroni) were performed to see whether there was a specific group of data that differed from the three data groups. This test showed no significant differences, therefore it can be concluded that no specific data group differed from the data groups.

5. Overview of the tested hypotheses

Figure 6 provides an overview of the tested hypotheses and shows whether they are confirmed or rejected, based on the results of the experiment. The red arrow indicates that the hypothesis is rejected and the green arrow indicates that the hypothesis is confirmed.

In addition, three new lines have been added in this model compared to the original conceptual model (Figure 3). These lines were not hypothesized in the literature section, but have been added based on the outcomes of the experiment. The first line shows a positive relation between familiarity and online privacy protection behavior. The second line shows a negative relation between uncertainty and online privacy protection behavior. The third line shows a positive relation between quick decision and online privacy protection behavior.

These added lines and the rejected or confirmed hypotheses will be discussed further in the discussion chapter.

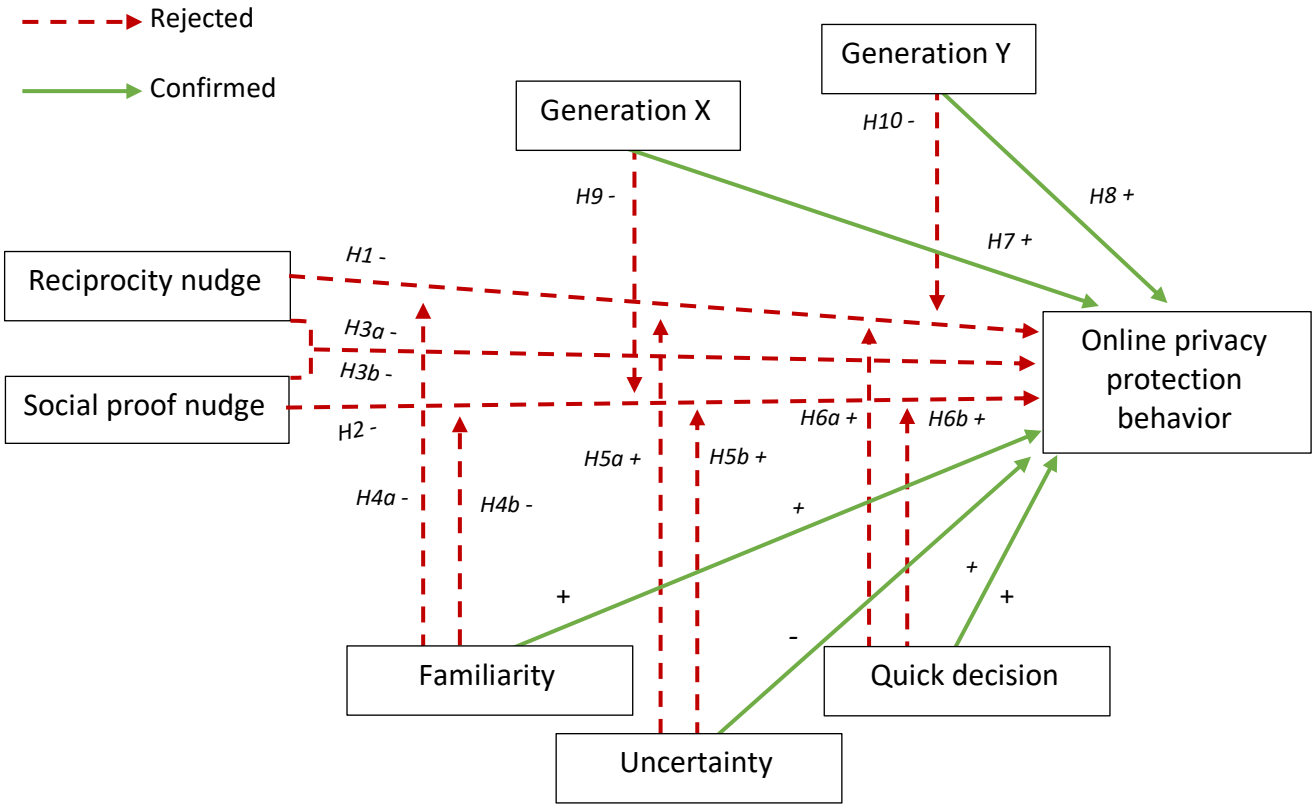

Figure 6. Overview of tested hypotheses

6. Discussion

The discussion chapter focuses on elaborating on the main findings and general discussion, limitations and future research, and the conclusion.

6.1. Main findings and general discussion

The present study investigated to what extent social proof and reciprocity nudges can influence the online privacy protection behavior of Generation X and Generation Y. The results showed that the nudges had no effect on participants' online privacy protection behavior. Moreover, generations showed no effect on the nudges. However, familiarity, uncertainty and quick decision were important predictors of participants' online privacy protection behavior.

Familiarity, uncertainty and quick decision

The familiarity, uncertainty and quick decision regarding the real corona-app in development (CoronaMelder) were analyzed. Based on the results, most of the participants in the experiment had a high level of familiarity, uncertainty and quick decision regarding the corona-app. When it comes to the interaction effect, no interaction effect was found between the nudges, generations, familiarity, uncertainty, and quick decision. However, the study found main effects of familiarity, uncertainty and quick decision on the online privacy protection behavior. These main effects will be further discussed.

The literature section did not mention the effect of familiarity on online privacy protection behavior, but the results showed some interesting outcomes. In the manipulations section (3.4), it was suggested that participants would have a low level of familiarity because the corona-app did not yet exist in the Netherlands. However, the experiment took place from 13 to 23 July 2020. During this period much was known about the corona-app because the University of Twente was fully testing the final version of the app and it was mentioned in the news (University of Twente, 2020). Therefore, it is not a surprising outcome that participants had a high level of familiarity. The results showed that there was a main effect of familiarity on online privacy protection behavior; people with a high level of familiarity showed less online privacy protection behavior than people with a low level of familiarity. A previous study by Lee and Kwon (2011) explains that familiarity with a website results in a feeling of intimacy that encourages the self-disclosure of personal information. They state that there is a positive relationship between familiarity and good feelings about a website. If we translate this to this study, it can be concluded that people with high familiarity with the corona-app felt good about the app which reduced their online privacy protection behavior. Moreover, this finding explains why familiarity is more predictable for online privacy protection behavior than the two nudges in this study. If there is familiarity, it does not matter what form of nudge is added, it will not influence the online privacy protection behavior. Nudges may therefore no longer be effective if people are familiar with the corona-app, which explains why the nudges had no effect.

Moreover, the literature section did not include the effect of uncertainty on online privacy protection behavior but the results provided interesting outcomes. In line with the suggestion in the manipulation section (3.4), participants had a high level of uncertainty because there have been many personal data leaks from previous versions of the app. Furthermore, the results showed that there was a main effect of uncertainty on online privacy protection behavior; people with a high level of uncertainty showed more online privacy protection behavior compared to people with a low level of uncertainty. Gambino et al. (2016) state that new or unfamiliar technologies raise user concerns about information sharing. Moreover, people feel immediate discomfort with the unknown technology. In

addition, Gambino et al. (2016) found that uncertainty is a negative heuristic that inhibits information disclosure behavior leading to the privacy paradox. This uncertainty heuristic refers to situations where people feel unsafe because of their lack of understanding of the technology. Translating this to this study, people felt unsafe or uncertain about using the corona-app because the app had not yet been launched, therefore they had a lack of understanding the app. It can be concluded in the present study that people with a high feeling of uncertainty about the corona-app inhibited information disclosure, which increased their online privacy protection behavior. Moreover, this finding explains why uncertainty is more predictable for online privacy protection behavior than the nudges. When people are uncertain about the corona-app, a nudge can no longer influence their online privacy protection behavior. Therefore, the nudges had no effect.

Further, the effect of quick decision on online privacy protection behavior was not mentioned in the literature section but the results provided some interesting outcomes. It was stated in the manipulation section (3.4) that people would have a high level of quick decision regarding the corona-app because the app needs to be accepted rapidly to maximize the effect of the app by preventing the spread of the coronavirus. This suggestion was confirmed by the results. The results showed that there was a main effect of quick decision on online privacy protection behavior; people with a high level of quick decision showed less online privacy protection behavior than people with a low level of quick decision. When people have to make a quick decision in a limited time, they cannot make rational choices. In context of this study, people had to decide within a limited time frame whether to use the app, as it was stated that most of the Dutch should use the app as soon as possible to prevent the spread of the virus. A review of current research on privacy paradox phenomenon by Kokolakis (2017) shows that when people have to make privacy decisions within a limited time frame, they have incomplete information about the risks and benefits. Therefore, it can be concluded that people with a high level of quick decision did not make rational choices because they had incomplete information about the risks and benefits of the corona-app. It can therefore be assumed that people with a high level of quick decision have based their online privacy protection behavior on the main goal of the corona-app, which is to limit the spread of the coronavirus. Therefore, people with a high level of quick decision showed less online privacy protection behavior than people with a low level of quick decision. Moreover, this finding explains that quick decision is more predictable for online privacy protection behavior than the nudges. Nudges may therefore no longer be effective if people are making a quick decision regarding the corona-app, which explains why the nudges had no effect.

In the context of the corona-app, the media played a role in participants' level of familiarity, uncertainty and quick decision. The real corona-app in development (CoronaMelder), was mentioned frequently in the news. The news is able to influence the salience of the topics and their images among people, which is called the agenda-setting role of the news media (McCombs & Reynolds, 2002). The agenda-setting theory states that the salience of subject on the news agenda influences their salience on the public agenda. This starts with the agenda of subjects that gets prominent attention in the news. The subject is the thing we have an opinion about (Carroll & McCombs, 2003). At the time of writing this study, the salience and image of the corona-app were affected by the news. The news gave the corona-app and it privacy aspects prominent attention, which caused people to become familiar with the app. In addition, the news explained that the privacy of the corona-app users was still insufficiently guaranteed, which caused people to become uncertain about using the app. Furthermore, the news stated that the corona-app had to be made available for the Dutch as soon as possible to prevent the spread of the virus, which caused that people were willing to make a quick decision about using the app (RTL Nieuws, 2020).

Online privacy protection behavior

The results of the experiment further showed that participants in all manipulations showed online privacy protection behavior, both on the internet and in the fictional corona-app interface, because participants scored higher than average on online privacy protection behavior. However, there was a difference between online privacy protection on the internet and in the fictional corona-app interface; participants' online privacy protection behavior in the fictional corona-app was higher than on the internet. Since the privacy protection behavior in the fictional corona-app was higher than on the internet, it is expected that people were too environmentally sensitive to properly test the nudges. Boun My and Ouvard (2019) found that the response to the nudge directly depends on people's environmental sensitivity. Etner et al. (2007, 2009) found that people's sensitivity determine their optimism regarding the risk of an environment. The most optimistic people, being the least sensitive, would contribute less to an environment than the least optimistic people, being the most sensitive. This would mean that in this study, people with low sensitivity to the corona-app would be highly optimistic concerning the privacy risks the app, as the corona-app is not a priority for them. It is likely that people were environmentally sensitive since the coronavirus is currently spreading worldwide. Therefore, people already have a certain feeling and idea about the corona-app, making it more difficult to influence their behavior through a subtle nudge. Moreover, it is likely that the risk of the app is emphasized by the privacy data (health data, personal data and location data) that people have to accept in order to use the app.

For this study, a corona-app interface was designed where participants were asked to accept three different kinds of private data (health data, personal data and location data) to use the corona-app. The health data and location data did not score higher than average acceptance that the corona would use these data. Personal data scored even less than average acceptance. This may have resulted in the online privacy protection behavior of participants in the fictional corona-app being higher than in general on the internet. This is very plausible given that the Netherlands introduced the General Data Protection Regulation (GDPR) in May 2018. This law has strengthened and expanded people's privacy rights (Ministerie van Justitie, 2018). This legislative change was frequently mentioned in the news at the time. In addition, Autoriteit Persoonsgegevens (2019), or in English the Dutch Data Protection Authority (DPA), makes Dutch people aware that it is their choice to share private data. Therefore, it is likely that people have become more aware of their privacy data and their privacy rights. Moreover, based on participants' reasons for being (un)willing to accept that the corona-app used this private data, it can be concluded that they did not make their decision based on the nudge. Rather, they based their decision on what they think about this kind of private data and the corona-app. It can further be questioned whether participants noticed the nudge at all, because they did not mention it in their keyword reasons. The salience of the nudge has been tested in preliminary research. However, based on the results of the preliminary test, the fictional corona-app interface has undergone several adjustments. These adjustments may have caused that participants did not notice the nudge or may have deterred participants due to the kind of private data they had to accept.

Online privacy protection behavior and generations

Furthermore, focusing on the generations, the results showed that Generation X and Generation Y both showed online privacy protection behavior on the internet and in the fictional corona-app. This result is in line with the literature section which states that Generation X and Generation Y both show high online privacy protection behavior due to their high level of online privacy concerns (Ruigrok NetPanel, 2019). Moreover, the results showed that Generation X showed more online privacy protection behavior on the internet

compared to Generation Y. This is not an unexpected outcome since it was stated in the literature that Generation X (45.5%) has slightly more privacy concerns on the internet than Generation Y (43.9%) (Ruigrok NetPanel, 2019). The results further show that when it comes to the fictional corona-app, there was no difference between the generations regarding their online privacy protection behavior. As mentioned above, the differences are very small between generations and their online privacy protection behavior. Therefore, it was expected that there would be no differences.

Online privacy protection behavior and nudges

The study aimed to clarify to what extent social proof and reciprocity nudges can influence the online privacy protection behavior of Generation X and Generation Y. According to the results, the main effect of the social proof nudge and reciprocity nudge on participant's online privacy protection behavior was not found. Further, no interaction effect was found between the two nudges. Moreover, there was no main effect of generations on online privacy protection behavior. In addition, there was no interaction effect found between the two nudges and generations. What is striking about all the results of the experiment is that none of the expectations regarding the two nudges was supported. The question is therefore whether the two nudges actually were effective in the experiment. This section discusses additional literature to learn more about the two nudges and online privacy protection behavior. In his research on solving the privacy paradox, Baek (2014) found that the dichotomy between privacy concerns and behavioral intentions disappears when people are presented with arguments to disclose their private information online. Moreover, since the privacy paradox stems from people's lack of thoughtful consideration when forming opinions about the online privacy problem, the paradox should go away when people are being exposed to the relevant arguments to disclose their private date. According to the literature, a nudge is a subtle hint that can have behavioral effect (Workwire, 2015). Based on the characteristics of Generation X, the social proof nudge was used in this study. Buck et al. (2014) showed that people consider information from their social group to be more important and reliable than information provided by application vendors about the use of personal data. Moreover, Klumpe et al. (2018) found that social proof increases people's trusting beliefs. In addition, the presence of social proof cancels out the negative effects of privacy concerns. Based on these additional findings, the presence of a social proof nudge should be more negatively related to online privacy protection behavior compared to the absence of a social proof nudge. Further, based on the characteristics of Generation Y, the reciprocity nudge was used in the study. Various theories already considered the effect of reciprocity on privacy behavior. The rational choice theory by Simon (1995) states that decisions are being made to achieve the greatest benefit or satisfaction in accordance with people's perceived self-interest. When making decisions, people seek to maximize utility and minimize risks. In the online environment, people base their decision-making for information disclosure on perceived benefits (e.g. networking) and perceived risks (e.g. privacy). According to the privacy calculus theory, the perceived benefits outweigh the perceived risks, leading to neglecting the privacy concerns that result in the disclosure of information in exchange for benefits (Culnan & Armstrong, 1999). Based on these theories, the presence of a reciprocity nudge should be more negatively related to online privacy protection behavior compared to the absence of a reciprocity nudge. Both the additional literature and the literature presented in the literature section confirm the expectations and do not explain why these nudges did not work as previously expected. This may be related to the fictional corona-app created for this empirical study. It is striking that most participants would use the corona-app if it existed, but their online privacy behavior in the fictional corona-app was very high. More specific, while the literature section claimed it would be the other way

around, participant's online privacy protection behavior in the fictional corona-app was higher than on the internet.

In addition to the findings in the experiment, it can be questioned whether the nudges were worded strongly enough to be effective. The wording of the nudges was based on the input from preliminary research. The reciprocity nudge was formulated from the idea that people get something in return. However, Sunstein (2016) states that people dislike losses more than they like gains. When reciprocity was formulated with a loss instead of a gain, it could have had a greater effect. In addition, it can be questioned whether the formulated reciprocity nudge actually fits with reciprocity. The actual formulation of the nudges was established in preliminary research. During this research, people were told what reciprocity entailed and in an open discussion they were asked whether they could formulate an attractive reciprocity nudge. However, it turned out not to be useful to have people who are not experts formulate a reciprocity nudge themselves. This could explain why the reciprocity nudge had no effect in this study. Moreover, formulating a reciprocity nudge in the corona-app context is difficult because of the social aspects of the app. As formulated in the literature section, many studies show that monetary gifts can effectively trigger reciprocity (Berry & Kanouse, 1987; Roethke et al., 2020; Acquisti et al., 2013). If these monetary gifts would be used to influence the online privacy protection behavior in the fictional corona-app, people would be motivated by the financial aspect which unethically affects their voluntary participation in the app (Verbeek et al., 2020). For gifts where the social function is dominant, money is far from ideal and may be very unacceptable (Webley et al., 1983). Since the corona-app is conducted from a social point of view, it would be unacceptable to use monetary gifts in this context. Therefore, the reciprocity nudge in this study was not based on monetary gifts, but rather on people's health and the social aspects. When people know they have been in contact with others infected with the coronavirus, they can protect the health of those around them by going into quarantine. Furthermore, the social proof was formulated based on the norms of the Dutch society. Halpern (2016) found that social norms can only change behavior if they are the norms of a particular community, not the nation as a whole. If the social proof nudge in this study used a more specific group people, the nudge could have a greater effect. Moreover, a study by Sunstein (2016) about nudges that fail, explains that a nudge is not a good idea for those who were unaffected by the nudge. When people ignore or reject the nudge, it is because they know best. This is diagnostic in the sense that this shows that people act in accordance with their feelings. When people do not reduce their online privacy protection behavior because they know how the corona-app affects their privacy, a nudge will not persuade them to do so.

Discussion of findings on nudges

In sum, it can be questioned whether the nudges were not effective because people were familiar, uncertain and wanted to make a quick decision regarding the corona-app. Moreover, it can be questioned whether people were too focused on the privacy data, people did not notice the nudges, people were too environmentally sensitive or because the nudges were not formulated attractively enough to be effective. This would explain why both nudges did not work as predicted by the literature. More specific, it would explain why the nudges did not reduce the online privacy protection behavior and explains why there was no interaction effect between the two nudges. In addition, it explains why it prevented the effect of the two nudges from being strengthened or weakened by familiarity, uncertainty and quick decision. Moreover, because the nudges were not effective, it can be argued why there is no different effect of the nudges on Generation X and Generation Y.

6.2. Limitations and future research

When interpreting the study results, several limitations should be acknowledged. To start with, a limitation of this study is the environment where the nudges were tested. The study used a fictional corona-app interface with three kinds of private data that participants needed to accept in order to use the app. It can be questioned whether this kind of private data was not too private for the use of the corona-app based on the degree of acceptance of the private data. If the private data only included health data and location data, people's online privacy protection behavior in the fictional corona-app interface could be lower. In addition, they might be less deterred, increasing the salience and the effect of the nudge. Moreover, the results of this study showed that the fictional corona-app gave people a high feeling of uncertainty. If an environment entails a high level of quick decision and familiarity, and a low level of uncertainty, people's online privacy protection behavior would be lower. In addition, results have shown that people could be environmentally sensitive for the corona-app. Moreover, as mentioned in the discussion, the corona-app context did not lend itself well to properly test the reciprocity nudge. Therefore, a more natural environment could test the nudges more properly and could lead to different results.

The study included a preliminary test. However, given the various adjustments in the fictional corona-app interface, a second preliminary test should have been carried out to measure the effect of the nudges and the fictional corona-app itself. If the second preliminary test had been carried out, the effect of the nudge could have been greater and participants' online privacy protection behavior in the app could have been lower.

In addition, the formulation of the nudges was based on preliminary research. As discussed, the procedure for formulating the nudges is questionable. Rather than discussing the wording of the nudges in an open discussion, the researcher should have shown people three different wording of the nudges that actually fit with reciprocity. In that case, people could have chosen between these three formulations and the most frequently mentioned formulation of the nudge could have been used in the experiment.

As mentioned in the discussion, the salience of de nudges is questioned. If eye-tracking equipment was used in the study, the noticing of the nudges could be better tested because this equipment could be used to investigate what people are looking at when seeing the privacy notification in the fictional corona-app. Moreover, it could have been tested whether participants noticed the nudges at all.

Overall, it can be questioned whether this study is ethical. Many might argue that it is unethical to nudge someone to reduce their online privacy protection behavior. However, under certain circumstances it is important to reduce people's online privacy protection behavior to make sure that they start using, in this case, the corona-app as it is important for health and society. As previously mentioned, according to the Ministerie van Algemene Zaken (2020), or in English the Dutch Ministry of General Affairs, 60% of the Dutch must use the corona-app to ensure that it is effective in preventing the spread of the virus. Therefore, this study applies the concept of nudging to make people feel safer through the positive side of the corona-app in the hope that, by formulating the importance of the corona-app, decision makers would choose a safer and more informed option. After conducting the experiment in this study, an expert panel conducted an ethics analysis and identified and investigated ten ethical issues related to the corona-app (Verbeek et al., 2020). One of their recommendations was that the use of the app must be completely voluntary. The expert panel states in their ethical recommendations that no incentives should be given that make people feel compelled to use the corona-app. Since nudges are referred as subtle incentives, it is not ethical to use nudges in the corona-app. This study did use nudges in a fictional corona-app to reduce people's online privacy protection behavior, which is a limitation of the study.

Moreover, privacy is a known ethical issue of the corona-app. The expert panel states that the corona-app must respect the privacy of users. However, the fictional corona-app in this study used people's personal data, health data and location data. This fictional version of the corona-app is therefore unethical, which is another limitation of the study.

When it comes to future research, several new questions have emerged from this study. Firstly, a new question could be whether other types of nudges can change the online privacy protection behavior of Generation X and Generation Y. Secondly, a new question could be whether a different environment can properly test the nudges and change the online privacy protection behavior of Generation X and Generation Y. Further, it could be interesting to research whether other generations could be included in research into the effect of nudges on online privacy protection behavior. In addition, it could be tested whether other provinces of the Netherlands reveal a different outcome for the research into nudges that influence the online privacy protection behavior of Generation X and Generation Y. Finally, for future research it would be useful to test the salience of nudges with eye-tracking.

6.3. Conclusion

The present study shows that the social proof nudge and reciprocity nudge did not influence the online privacy protection behavior of Generation X and Generation Y. This can be concluded from the various obtained results from the experiment:

- The study shows that familiarity, uncertainty and quick decision had an effect on online privacy protection behavior. People who were familiar with the corona-app (CoronaMelder) and were willing to make a quick decision about using this app showed less online privacy protection behavior in the fictional corona-app compared to people who were unfamiliar and were not willing to make a quick decision regarding the corona-app. People who were uncertain about using the corona-app (CoronaMelder) showed more online privacy protection behavior in the fictional corona-app compared to people who were certain about using the corona-app. Familiarity, uncertainty and quick decision had no effect on the relationship between the nudges and online privacy protection behavior.

- All people showed online privacy protection behavior both on the internet and in the fictional corona-app. However, their online privacy protection behavior in the fictional corona-app was higher than on the internet. All people accepted that the fictional corona-app used their location data, and health data, but unaccepted that the app used their personal data.

- Generation X showed more online privacy protection behavior on the internet than Generation Y. Both Generation X and Generation Y showed online privacy protection behavior in the fictional corona-app.

- The social proof nudge and reciprocity nudge had no effect on online privacy protection behavior and the two nudges did not interact with each other. Generations had no effect on online privacy protection behavior and generations had no effect on the relationship between the nudges and online privacy protection behavior.

In short, the current study has contributed to the existing literature about the influence of nudges on the online privacy protection behavior of Generation X and Generation Y. The study specifically focused on the effect of the social proof nudge and reciprocity nudge. Although the results have not shown the expected effect of the two nudges on online privacy protection behavior and the difference between Generation X and Generation Y, it has shown that Generation X and Generation Y both showed online privacy protection behavior. The study further established a direct effect of familiarity, uncertainty and quick decision on online privacy protection behavior. Therefore, online platforms can lower the online privacy protection behavior of Generation Y and Generation Y by ensuring that they have a high level of familiarity and quick decision, and a low level of uncertainty regarding the online platform.

References

Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE security & privacy*, *7*(6), 82-85.

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose. *Journal of Marketing Research*, *49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., Wilson, S. (2017). Nudges for Privacy and Security. *ACM Computing Surveys*, *50*(3), 1–41. https://doi.org/10.1145/3054926

AudienceData. (2018, June 7). *Generation segments*. Retrieved from https://www.audiencedata.com/generation-segments/

Autoriteit Persoonsgegevens. (2019, January 28). *Nederland maakt zich zorgen over privacy*. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/nederland-maakt-zich-zorgen-over-privacy

Autoriteit persoonsgegevens. (2020, April 17). *AP toetst opzet corona-apps*. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-toetst-opzet-corona-apps

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior*, *38*, 33–42. https://doi.org/10.1016/j.chb.2014.05.006

Bar-Anan, Y., Wilson, T. D., & Gilbert, D. T. (2009). The feeling of uncertainty intensifies affective reactions. *Emotion*, *9*(1), 123–127. https://doi.org/10.1037/a0014607

Berry, S. H., & Kanouse, D. E. (1987). Physician Response to a Mailed Survey an Experiment in Timing of Payment. *Public Opinion Quarterly*, *51*(1), 102. https://doi.org/10.1086/269018

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*. https://doi.org/10.1177/0093650218800915

Boun My, K., & Ouvrard, B. (2019). Nudge and tax in an environmental public goods experiment: Does environmental sensitivity matter? *Resource and Energy Economics*, *55*, 24–48. https://doi.org/10.1016/j.reseneeco.2018.10.003

Brehm, J. W. (1966). *A theory of psychological reactance.* Academic Press.

Buck, C., Horbel, C., Germelmann, C.C., & Eymann, T. (2014). The Unconscious App Consumer: Discovering and Comparing the Information-seeking Patterns among Mobile Application Consumers. *ECIS*.

Carroll, C. E., & McCombs, M. (2003). Agenda-setting Effects of Business News on the Public's Images and Opinions about Major Corporations. *Corporate Reputation Review*, *6*(1), 36–46. https://doi.org/10.1057/palgrave.crr.1540188

Cialdini, R.B. (2009). *Influence: The Psychology of Persuasion*. HarperCollins Publishers Inc.

Cialdini, R. B. (2017). *Pre-Suasion: A Revolutionary Way to Influence and Persuade*. Random House Business.

Clee, M. A., & Wicklund, R. A. (1980). Consumer Behavior and Psychological Reactance. *Journal of Consumer Research*, *6*(4), 389. https://doi.org/10.1086/208782

Cohen, I., Brinkman, W. P., & Neerincx, M. A. (2012). Assembling a synthetic emotion mediator for quick decision making during acute stress. *Proceedings of the 30th European Conference on Cognitive Ergonomics*, 9–12. https://doi.org/10.1145/2448136.2448182

Consumentenbond. (2020, October 21). *Corona-app: privacy is een must*. Retrieved from https://www.consumentenbond.nl/internet-privacy/privacyvriendelijke-corona-app-een-must

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104 115. https://doi.org/10.1287/orsc.10.1.104

Dainton, M., & Zelley, E. D. (2014). *Applying Communication Theory for Professional Life*. United States: Sage Publications Inc.

Didenko, L. (2016, March 22). Nudging: onbewust gedrag bewust beïnvloeden. Retrieved from https://www.marketingfacts.nl/berichten/nudging-onbewust-gedrag-bewust-beinvloeden

Etner, J., Jeleva, M., & Jouvet, P.A. (2007). Risk perceptions, voluntary contributions and environmental policy. *Research in Economics*, *61*(3), 130–139. https://doi.org/10.1016/j.rie.2007.05.001

Etner, J., Jeleva, M., & Jouvet, P. A. (2009). Pessimsim or optimism: A justification to voluntary contributions toward environmental quality. *Australian Economic Papers*, *48*(4), 308–319. https://doi.org/10.1111/j.1467-8454.2009.00378.x

Franklin, M., Folke, T., & Ruggeri, K. (2019). Optimising nudges and boosts for financial decisions under uncertainty. *Palgrave Communications*, *5*(1). https://doi.org/10.1057/s41599-019-0321-y

Gambino, A., Kim, J., Sundar, S. S., Ge, J., & Rosson, M. B. (2016). User Disbelief in Privacy Paradox: Heuristics that determine Disclosure. *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '16*, 2837–2843. https://doi.org/10.1145/2851581.2892413

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, *28*(6), 725–737. https://doi.org/10.1016/s0305-0483(00)00021-9

Glass, A. (2007). Understanding generational differences for competitive success. *Industrial and Commercial Training*, *39*(2), 98–103. https://doi.org/10.1108/00197850710732424

Gurău, C. (2012). A life-stage analysis of consumer loyalty profile: comparing Generation X and Millennial consumers. *Journal of Consumer Marketing*, *29*(2), 103–113. https://doi.org/10.1108/07363761211206357

Halpern, D. (2016). *Inside the Nudge Unit*. Virgin Digital.

Hofstede, G. (1991). *Cultures and organizations: Software of the mind*. London: McGraw-Hill.

Howe, N., & Strauss, W. (2009). *Millennials Rising: The Next Great Generation*. Vintage.

Hsu, S. F., & Shih, D. H. (2009). The factors influencing individual's behavior on privacy protection. *WSEAS Transactions on Information Science and Applications*, *6*(9), 1591-1600.

Jäger, T., & Eisend, M. (2013). Effects of Fear-Arousing and Humorous Appeals in Social Marketing Advertising: The Moderating Role of Prior Attitude Toward the Advertised Behavior. *Journal of Current Issues & Research in Advertising*, *34*(1), 125–134. https://doi.org/10.1080/10641734.2013.754718

Jung, J. M., & Kellaris, J. J. (2004). Cross-national differences in proneness to scarcity effects: The moderating roles of familiarity, uncertainty avoidance, and need for cognitive closure. *Psychology and Marketing*, *21*(9), 739–753. https://doi.org/10.1002/mar.20027

Klumpe, J., Koch, O. F., & Benlian, A. (2018). Correction to: How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets*, *30*(3), 587–588. https://doi.org/10.1007/s12525-018-0324-3

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

KPMG. (2017). *The truth about online consumers 2017 Global Online Consumer Report*. Retrieved from https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/01/the-truth-about-online-consumers.pdf

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, *41*(1), 127-149.

Lee, Y., & Kwon, O. (2011). Intimacy, familiarity and continuance intention: An extended expectation–confirmation model in web-based services. *Electronic Commerce Research and Applications*, *10*(3), 342–357. https://doi.org/10.1016/j.elerap.2010.11.005

Lissitsa, S., & Kol, O. (2016). Generation X vs. Generation Y – A decade of online shopping. *Journal of Retailing and Consumer Services*, *31*, 304–312. https://doi.org/10.1016/j.jretconser.2016.04.015

Liu, C.-W., Hsieh, A.-Y., Lo, S.-K., & Hwang, Y. (2017). What consumers see when time is running out: Consumers' browsing behaviors on online shopping websites when under time pressure. *Computers in Human Behavior*, *70*, 391–397. https://doi.org/10.1016/j.chb.2016.12.065

Luhmann, N. (2017). *Trust and Power*. Amsterdam, Netherlands: Amsterdam University Press.

Mann, M. F., & Hill, T. (1984). Persuasive communications and the boomerang effect: Some limiting conditions to the effectiveness of positive influence attempts. *ACR North American Advances*, *11*(1), 66-70.

Mannheim, K. (1970). The problem of generations. *Psychoanalytic review*, *57*(3), 378-404.

McCombs, M., & Reynolds, A. (2002). *News influence on our pictures of the world.* In J. Bryant & D. Zillmann (Eds.), *LEA's communication series. Media effects: Advances in theory and research* (p. 1–18). Lawrence Erlbaum Associates Publishers.

Michalek, G., Meran, G., Schwarze, R., & Yıldız, Ö. (2016). Nudging as a new "soft" policy tool: An assessment of the definitional scope of nudges, practical implementation possibilities and their effectiveness. *Economics discussion papers, no 2016-18Kiel:* Institute for the World Economy. Retrieved from http://www.economics-ejournal.org/economics/discussionpapers/2016-18/

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Ministerie van Algemene Zaken. (2020, November 17). *Coronavirus-apps*. Retrieved from https://www.rijksoverheid.nl/onderwerpen/coronavirus-app

Ministerie van Justitie. (2018, June 4). *Privacy en persoonsgegevens*. Retrieved from https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens

Molm, L. D., Collett, J. L., & Schaefer, D. R. (2007). Building Solidarity through Generalize Exchange: A Theory of Reciprocity. *American Journal of Sociology*, *113*(1), 205–242. https://doi.org/10.1086/517900

Multon, K. D., & Coleman, J. S. M. (2012). Coefficient Alpha. *Encyclopedia of Research Design*, 160–163. https://doi.org/10.4135/9781412961288.n53

Palfrey, J., & Gasser, U. (2013). *Born digital: Understanding the first generation of digital natives.* New York: Basic Books.

Papp, R., & Matulich, E. (2011). Negotiating the deal: Using technology to reach the millennials. *Journal of Behavioral Studies in Business*, *4*, 1.

Parelta, E. (2015, September 17). *Generation X: The Small But Financially Powerful Generation*. Retrieved from https://www.centro.net/blog/generation-x-the-small-but-mighty-generation

Park, C. W., & Lessig, V. P. (1981). Familiarity and Its Impact on Consumer Decision Biases and Heuristics. *Journal of Consumer Research*, *8*(2), 223. https://doi.org/10.1086/208859

Parment, A. (2013). Generation Y vs. Baby Boomers: Shopping behavior, buyer involvement and implications for retailing. *Journal of Retailing and Consumer Services*, *20*(2), 189-199. https://doi.org/10.1016/j.jretconser.2012.12.001

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2019). Nudge Me Right: Personalizing Online Nudges to People's Decision-Making Styles. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3324907

Psychology Today. (2018, March 21). Persuasion. Retrieved from https://www.psychologytoday.com/us/basics/persuasion

Raue, M., Scholl, S.G. (2018). The Use of Heuristics in Decision Making under Risk and Uncertainty. In M. Raue, E. Lermer & B. Streicher (Eds.), *In Psychological Perspectives on Risk and Risk Analysis: Theory, Models and Applications* (pp. 153-179). New York, NY: Springer.

Reisenwitz, T. H., & Iyer, R. (2009). Differences in Generation X and Generation Y: Implications For The Organization And Marketers. *Marketing management journal*, *19*(2).

Roethke, K., Klumpe, J., Adam, M., & Benlian, A. (2020). Social influence tactics in e commerce onboarding: The role of social proof and reciprocity in affecting user registrations. *Decision Support Systems*, *131*, 113268. https://doi.org/10.1016/j.dss.2020.113268

RTL Nieuws. (2020, August 18). *Corona-app in de top van de appwinkels ondanks kritiek privacyautoriteit*. Retrieved from https://www.rtlnieuws.nl/tech/artikel/5177936/corona-app-coronamelder-downloads-kritiek-autoriteit-persoonsgegevens

Ruikrok NetPanel. (2019, May 22). *What's Happening Online in 2019?* Retrived from https://www.ruigroknetpanel.nl/ruigrok-netpanel/whats-happening-online-in-2019/

Salahuddin, M. M. (2010). Generational Differences Impact On Leadership Style And Organizational Success. *Journal of Diversity Management*, *5*(2). https://doi.org/10.19030/jdm.v5i2.805

Schneider, D., Klumpe, J., Adam, M., & Benlian, A. (2019). Nudging users into digital service solutions. *Electronic Markets*, *30*(4), 863–881. https://doi.org/10.1007/s12525-019-00373-8

Simon, H. A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, *69*(1), 99. https://doi.org/10.2307/1884852

Smola, K. W., & Sutton, C. D. (2002). Generational differences: revisiting generational work values for the new millennium. *Journal of Organizational Behavior*, *23*(4), 363–382. https://doi.org/10.1002/job.147

Sunstein, C. R. (2016). Nudges that fail. *Behavioural Public Policy*, *1*(1), 4–25. https://doi.org/10.1017/bpp.2016.3

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions about Health, Wealth and Happiness.* New Haven, CT: Yale University Press.

Twenge, J. M. (2014). *Generation Me*. Amsterdam, Netherlands: Adfo Books.

University of Twente. (2020, August 6). *Ethical test: final phase corona-app testing*. Retrieved from https://www.utwente.nl/en/news/2020/8/727647/ethical-test-final-phase- corona-app-testing#testing-the-corona-notification-app-in-twente

Van Kempen, H. (2017, April 21). Nudging. Retrieved from https://toezichtkennis.pleio.nl/pages/view/49220682/nudging

Verbeek, P. P. C. C., Brey, P., van Est, R., van Gemert, L., Heldeweg, M., & Moerel, L. (2020, July 14). *Ethische analyse van de COVID-19 notificatie-app ter aanvulling op bron en contactonderzoek GGD*. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2020/07/14/ethische-analyse-van-de-covid-19-notificatie-app-ter-aanvulling-op-bron-en-contactonderzoek-ggd

Verhiel, T. (2017). Het spel der generaties. *Tijdschrift voor de Politie*, *79*(4). Retrieved from https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/93646.pdf

Wai Kwan Leung, J., & Taylor, G. (2002). Fashion buying criteria of X Generation consumers in Hong Kong. *Journal of Fashion Marketing and Management: An International Journal*, *6*(1), 63–76. https://doi.org/10.1108/13612020210422473

Webley, P., Lea, S. E. G., & Portalska, R. (1983). The unacceptability of money as a gift. *Journal of Economic Psychology*, *4*(3), 223–238. https://doi.org/10.1016/0167-4870(83)90028-4

Weinmann, M., Schneider, C., & Brocke, J. vom. (2016). Digital Nudging. *Business & Information Systems Engineering*, *58*(6), 433–436. https://doi.org/10.1007/s12599016-0453-1

Whatley, M. A., Webster, J. M., Smith, R. H., & Rhodes, A. (1999). The Effect of a Favor on Public and Private Compliance: How Internalized is the Norm of Reciprocity? *Basic and Applied Social Psychology*, *21*(3), 251–259. https://doi.org/10.1207/s15324834basp2103_8

Workwire. (2015, June 14). 'Workplace nudging' persuades people to desirable behavior. Retrieved from https://www.workwire.nl/en/workplace-nudging/

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zhang, B., & Xu, H. (2016). Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16*, 1676–1690. https://doi.org/10.1145/2818048.2820073

Appendices

Appendix 1 – Condition 1 with social proof nudge and reciprocity nudge

Appendix 2 – Condition 2 with social proof nudge

Appendix 3 – Condition 3 with reciprocity nudge

Appendix 4 – Condition 4 without nudge (control group)

Appendix 5 – Questions preliminary test (in Dutch)

Ik ga onderzoek doen naar het online privacybeschermingsgedrag van mensen met betrekking tot de corona-app. De vragen die je nu zult beantwoorden zullen gebruikt worden voor mijn vooronderzoek. Ik zal dit gesprek opnemen, ga je hiermee akkoord?

De vraag waarmee ik zou willen beginnen is:
Kom je uit generatie X (1965 tot en met 1975) of generatie Y (1985 tot en met 1995)?

1e set vragen over de Social proof nudge
Voor het eerste deel van het vooronderzoek laat ik een afbeelding zien van een mogelijke interface van de corona-app waarbij je een privacy-melding te zien krijgt. Hier ga ik enkele vragen over stellen.

1. Kan je deze afbeelding goed in je opnemen en enkele steekwoorden benoemen die in je opkomen?
2. Wat valt je op aan deze afbeelding?
3. Zou je bij het zien van deze melding je privacy beschermen en niet op ‘oke’ drukken of zal je op ‘oke’ drukken en je persoonlijke gegevens vrijgeven?
4. Kan je uitleggen waarom?
5. De schuingedrukte tekst is een vorm social proof, in het Nederlands ook wel bekend als sociale bewijskracht. Als je deze tekst zou mogen herformuleren zodat dat je eerder op ‘oke’ zal drukken bij het zien van de melding, hoe zou je dat dan doen?
6. Kan je uitleggen waarom je kiest voor deze herformulering van de melding en niet voor de huidige melding?

2e set vragen over de Reciprocity nudge

Voor het tweede deel van het vooronderzoek laat ik een andere afbeelding zien van een mogelijke interface van de corona-app waarbij je een privacy-melding te zien krijgt. Hier ga ik ook enkele vragen over stellen.

7. Kan je deze afbeelding goed in je opnemen en enkele steekwoorden benoemen die in je opkomen?
8. Wat valt je op aan deze afbeelding?
9. Zou je bij het zien van deze melding je privacy beschermen en niet op ‘oke’ drukken of zal je op ‘oke’ drukken en je persoonlijke gegevens vrijgeven?
10. Kan je uitleggen waarom?
11. De schuingedrukte tekst is een vorm reciprocity, in het Nederlands ook wel bekend als wederkerigheid wat inhoudt dat je de app wel zal gebruiken als je er iets voor terug krijgt. Als je deze tekst zou mogen herformuleren zodat dat je eerder op ‘oke’ zal drukken bij het zien van de melding, hoe zou je dat dan doen?
12. Kan je uitleggen waarom je kiest voor deze herformulering van de melding en niet voor de huidige melding?

3e set vragen over beide nudges

Voor het laatste deel van het vooronderzoek dien je terug te denken aan de twee formuleringen die je hebt gekozen. Hier ga ik enkele vragen over stellen.

13. Kan je aangeven bij welke van de twee formuleringen je op ‘oke’ zal drukken?
14. Kan je uitleggen waarom je kiest voor deze formulering en niet voor de andere formulering?

Dat waren mijn vragen! Bedankt voor jouw deelname aan mijn vooronderzoek!

Appendix 6 – Results of the preliminary test

Before the experiment took place, the preliminary test was conducted in which a total of eleven people participated. These eleven people consisted of five people from Generation Y and six people from Generation X of which one person is a cybersecurity expert. In addition to his participation in the preliminary test, this expert has also given his opinion on the interface of the corona-app.

Interesting results have been derived from the preliminary test. Firstly, all the people from Generation Y chose for the interface with the reciprocity nudge, which is in line with the formulated hypothesis. Furthermore, four of the six people from Generation X chose for the interface with the social proof nudge, which is also in line with the formulated hypothesis. In addition, some people have indicated that they would not use the corona-app because they do not believe in the outcome of the app. Therefore, the indication whether people would use the corona-app if it existed in the Netherlands, is added to the experiment because this could explain the different results of the study.

Furthermore, the preliminary test have shown that the current wording of the social proof nudge and the reciprocity nudge are not attractive enough for people to agree with the privacy notification. Ten out of eleven people did not start at the reformulation with 'did you know', therefore this will not be used in the experiment. Various reformulations of the nudges were mentioned in the preliminary test, but there is an overlap between these reformulations. To begin with, the majority of people find a percentage in the social proof nudge unattractive because it cannot be trusted. Further, the majority of people prefer a social proof nudge that focuses on the positive aspects. Based on these findings, the following Dutch formulation of the social proof nudge is used in the experiment: “De helft van de Nederlanders heeft alle vakjes aangevinkt. Werkt u ook mee? Samen krijgen we het coronavirus onder controle.” Moreover, the majority of the people prefer a reformulation of the reciprocity nudge that guarantees their own safety. Therefore, the following Dutch formulation of the reciprocity nudge is used in the experiment: “Door alle vakjes aan te vinken komt u te weten of u in contact bent geweest met andere personen die besmet zijn met het coronavirus.”

In addition, two of the eleven people did not mention the (color of the) nudge in what they have noticed about the image or in the keywords that first came to mind when they saw this image. It is striking that they looked at the image very briefly. To prevent people in the study from looking at the image briefly and possibly missing the nudge, the experiment clearly states that participants should take their time to view the entire image carefully.

Furthermore, half of the people indicated that they did not find the nudge attractive in the color red, because this looks threatening, screaming, compelling, too much and is associated with something negative. According to the cybersecurity expert, the nudge will work better visually, if it is green because then it is associated with something positive and something good. The cybersecurity expert further stated that it should be explained what privacy information is needed and what people need to do in order to accept that the app uses this information. This is added to the Dutch notification that is used in the experiment: “Om de app 'Stop Covid-19' volledig te laten functioneren worden de onderstaande gegevens gebruikt. Vink alle vakjes aan om dit te accepteren.
❑ Locatiegegevens ❑ Gezondheidsgegevens ❑ Persoonlijke gegevens.”

Appendix 7 – Questionnaire (in Dutch)

Beste deelnemer,

Mijn naam is Sanne Nijland. Ter afronding van de Master Communication Studies aan de Universiteit van Twente ben ik momenteel mijn Master Thesis aan het schrijven.

Tegenwoordig worden mensen online geconfronteerd met een toenemend aantal privacy beslissingen. Om deze reden wordt er onderzoek gedaan naar het online privacybeschermingsgedrag van mensen uit Generatie X en Generatie Y. De vragenlijst die u zult invullen heeft betrekking tot het onderzoek en zal ongeveer **7 minuten** van uw tijd in beslag nemen.

Het onderzoek bestaat uit een experiment waarin gevraagd wordt om *goed* naar een afbeelding te kijken van een fictieve interface van de corona-app. Vervolgens worden er vragen gesteld met betrekking tot deze afbeelding. Daarnaast krijgt u vragen over de Nederlandse corona-app die momenteel in ontwikkeling is en vragen over uw algemeen online privacybeschermingsgedrag op het internet. U dient geboren te zijn tussen 1965-1975 of 1985-1995 om deel te nemen aan dit onderzoek.

De gegeven antwoorden zullen volledig anoniem worden verwerkt en uitsluitend gebruikt worden voor mijn onderzoek. Uw deelname aan dit onderzoek is geheel vrijwillig en u mag zich op elk moment uit het onderzoek terugtrekken.

Voor vragen, opmerkingen of meer informatie kunt u contact opnemen met mij via s.h.nijland@student.utwente.nl.

Bij voorbaat wil ik u bedanken dat u deel wilt nemen aan mijn onderzoek, dit wordt zeer gewaardeerd!

Sanne Nijland

Ik heb de bovenstaande informatie gelezen en begrepen. Ik ga akkoord met mijn deelname aan dit onderzoek.

- Ik ga akkoord
- Ik ga niet akkoord

Deel 1: Demografische gegevens
Het eerste deel van de vragenlijst bevat vragen over uw demografische gegevens.

1. Tot welke van de volgende twee leeftijdscategorieën behoort u?
   - 1965 – 1975
   - 1985 – 1995

2. Wat is uw geslacht?
   - Man
   - Vrouw
   - Anders, namelijk: …

3. Wat is uw hoogst behaalde opleidingsniveau?
    - Basisonderwijs
    - Praktijkonderwijs
    - Voorbereidend middelbaar beroepsonderwijs (VMBO: LWOO, BBL, KBL, GL, MAVO)
    - Hoger algemeen voortgezet onderwijs (HAVO)
    - Voorbereidend wetenschappelijk onderwijs (VWO: Atheneum, Gymnasium)
    - Middelbaar beroepsonderwijs (MBO)
    - Hoger beroepsonderwijs (HBO)
    - Universiteit Bachelor diploma
    - Universiteit Master diploma
    - Anders, namelijk: …

4. In welke provincie woont u?
    - Noord-Holland
    - Zuid-Holland
    - Noord-Brabant
    - Utrecht
    - Limburg
    - Groningen
    - Friesland
    - Drenthe
    - Gelderland
    - Zeeland
    - Flevoland
    - Overijssel

Geef op een schaal van 1 (sterk mee oneens) tot 5 (sterk mee eens) aan in hoeverre u het eens bent met de volgende stelling:

5. Ik ben ervaren met het internet (sociale media, websites, online chats, E-mail, online games, etc.).
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

6. Hoeveel uur per dag maakt u gemiddeld gebruik van het internet (sociale media, websites, online chats, E-mail, online games, etc.)?
    - 0 uur per dag
    - 1 tot 3 uur per dag
    - 4 tot 6 uur per dag
    - Meer dan 6 uur per dag

Deel 2: Kennis en mening over de Nederlandse corona-app in ontwikkeling
De corona-app voorkomt de verspreiding van het coronavirus in Nederland. Deze app geeft aan of u in contact bent geweest met een persoon die besmet is met het virus. Op het moment dat dit gebeurd is kunt u voorzorgsmaatregelen nemen zoals in thuisquarantaine gaan. Het tweede deel van de vragenlijst gaat over uw kennis en mening over de corona-app die momenteel in ontwikkeling is en door de Nederlandse overheid in de toekomst mogelijk wordt geïntroduceerd.

Geef op een schaal van 1 (sterk mee oneens) tot 5 (sterk mee eens) aan in hoeverre u het eens bent met de volgende stellingen:

7. Ik ben bekend met de corona-app en weet precies wat deze app inhoudt.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

8. Ik ben bekend met de privacy aspecten van de corona-app en weet precies welke gevolgen dit heeft voor mijn privacy en vrijheid.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

9. Ik ben bekend met de risico's die verbonden zijn aan de corona-app en weet precies welke gevolgen dit heeft voor mijn privacy.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

10. Ik voel me onzeker over het gebruik van de corona-app wanneer ik niet weet welke uitkomst deze app biedt.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

11. Ik neem niet het risico om mijn privacy gegevens door de corona-app te laten gebruiken wanneer de uitkomst van deze app niet kan worden voorspeld.
    1. Sterk mee oneens
    2. Mee oneens
    6. Niet mee oneens/niet mee eens
    3. Mee eens
    4. Sterk mee eens

12. Ik voel me stressvol wanneer ik de gevolgen van het gebruik van de corona-app niet kan voorspellen.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

13. Om de verspreiding van het coronavirus in te perken kom ik tot een snelle beslissing om wel of niet gebruik te maken van de corona-app.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

14. 60% van de Nederlanders dient gebruik te maken van de corona-app om alle andere corona-maateregelen te vervangen en daarom kom ik tot een snelle beslissing om wel of niet gebruik te maken van de corona-app.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

15. Om erachter te komen of ik in contact ben geweest met personen die besmet zijn met het coronavirus kom ik tot een snelle beslissing om wel of niet gebruik te maken van de corona-app.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

Deel 3: De corona-app

Het derde deel van de vragenlijst gaat over een fictieve interface van de corona-app. Deze getoonde app-interface is NIET de huidige versie van de CoronaMelder (de daadwerkelijke corona-app).

Hieronder vindt u een afbeelding van een fictieve interface van de corona-app. Neem alstublieft de tijd om deze afbeelding in het geheel goed te bekijken voordat u doorgaat naar de vragen.

Hier wordt een blok met één van de vier condities getoond.

In hoeverre bent u bereid om de vakjes aan te vinken?

16. Locatiegegevens

0 25 75 100

17. Gezondheidsgegevens

0 25 75 100

18. Persoonlijke gegevens

0 25 75 100

19. Waarom bent u bereid of onbereid om de vakjes aan te vinken? Geef maximaal 3 steekwoorden.
    - Steekwoord 1: ……..
    - Steekwoord 2: ……..
    - Steekwoord 3: ……..

Geef op een schaal van 1 (sterk mee oneens) tot 5 (sterk mee eens) aan in hoeverre u het eens bent met de volgende stellingen:

20. Ik zou gebruik maken van deze corona-app.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

21. Deze corona-app voldoet aan mijn behoeften.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

22. Ik zou deze corona-app aanbevelen aan andere mensen.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

Hieronder wordt nogmaals de afbeelding getoond die u zojuist heeft bekeken. Hier zullen wederom enkele vragen over worden gesteld.

Hier wordt een blok met één van de vier condities getoond.

Geef op een schaal van 1 (sterk mee oneens) tot 5 (sterk mee eens) aan in hoeverre u het eens bent met de volgende stellingen:

23. Bij het zien van deze afbeelding geef ik een verzonnen naam of identiteit op in volgende stap van de app waar ik mijn persoonlijke gegevens moet invullen.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

24. Bij het zien van deze afbeelding verstrek ik onvolledige informatie over mijzelf in de volgende stap van de app waar ik mijn persoonlijk gegevens moet invullen.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

25. Bij het zien van deze afbeelding vraag ik iemand (bijvoorbeeld ouders of vrienden) om advies voordat ik alle vakjes aanvink en op ‘accepteren’ klik en mijn persoonlijke gegevens achterlaat.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

26. Bij het zien van deze afbeelding lees ik eerst de privacyverklaring van de app voordat ik alle vakjes aanvink en op ‘accepteren’ klik en persoonlijke gegevens achterlaat.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

27. Bij het zien van deze afbeelding gebruik ik een andere app die niet om mijn persoonlijke gegevens vraagt.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

28. Bij het zien van deze afbeelding verlaat ik de app en maak ik er geen gebruik van.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

Deel 4: Algemeen over online privacybeschermingsgedrag
Het vierde deel van de vragenlijst gaat over uw online privacybeschermingsgedrag op het internet in het algemeen.

Geef op een schaal van 1 (sterk mee oneens) tot 5 (sterk mee eens) aan in hoeverre u het eens bent met de volgende stellingen:

29. Als ik online mijn persoonlijke gegevens moet invullen geef ik een verzonnen naam of identiteit op.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

30. Als ik online mijn persoonlijke gegevens moet invullen verstrek ik onvolledige informatie over mijzelf.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee oneens
    5. Sterk mee eens

31. Als ik online mijn persoonlijke gegevens moet invullen vraag ik iemand (bijvoorbeeld ouders of vrienden) om advies.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

32. Als ik online mijn persoonlijke gegevens moet invullen lees ik eerst de privacyverklaring die op de website/app staat.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

33. Als ik online mijn persoonlijke gegevens moet invullen ga ik naar andere websites/apps die niet om mijn persoonlijke gegevens vragen.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

34. Als ik online mijn persoonlijke gegevens moet invullen verlaat ik de website/app en maak ik er geen gebruik van.
    1. Sterk mee oneens
    2. Mee oneens
    3. Niet mee oneens/niet mee eens
    4. Mee eens
    5. Sterk mee eens

Toestemming intrekken of bevestigen

Mogelijk heeft u tijdens deze vragenlijst te maken gehad met een nudge. Een nudge is een vorm van overtuigen en kan uw gedrag en antwoorden op vragen hebben beïnvloed. De nudge werd in groene tekst weergegeven in de fictieve interface van de corona-app. De vakjes 'locatiegegevens, gezondheidsgegevens en persoonlijke gegevens' in deze interface werden genudged met als doel dat u bereid zou worden om de vakjes aan te vinken en uw online privacybeschermingsgedrag te veranderen.

Nu u op de hoogte bent van deze informatie, wilt u uw aanvankelijke toestemming bevestigen of intrekken?

- Toestemming bevestigen: gebruik de gegeven antwoorden voor het onderzoek.
- Toestemming intrekken: verwijder de gegeven antwoorden.

Uw antwoorden zijn verstuurd!

Bedankt voor uw tijd en deelname aan mijn onderzoek. Indien u uw toestemming heeft bevestigd, dan worden uw antwoorden zorgvuldig en anoniem verwerkt. Indien u uw toestemming heeft ingetrokken, dan worden uw antwoorden verwijderd.

Voor vragen, opmerkingen of meer informatie kunt u contact opnemen met mij via s.h.nijland@student.utwente.nl.