NOVA IMS
Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

THE EFFECTS OF DATA ACCESS VULNERABILITY ON THE PERCEPTION OF TRUST

In the Hotel Industry

Alexandra Inês Correia Variz

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

THE EFFECTS OF DATA ACCESS VULNERABILITY ON THE PERCEPTION OF TRUST

by

Alexandra Inês Correia Variz

Dissertation presented as a partial requirement for obtaining the Master's degree in Information Management, with a specialization in Marketing Intelligence

Advisor: Professor Dr. Diego Costa Pinto

May 2020

ACKNOWLEDGEMENTS (OPTIONAL)

Quero agradecer ao meu orientador Professor Doutor Diego Costa Pinto pelo acompanhamento durante todo este processo bem como pelo suporte dado, sem o apoio e ensinamentos transmitidos, não seria possível terminar mais uma etapa.

Agradeço também à minha família, principalmente ao meu pai por todo o apoio durante esta fase, que me levou a nunca desistir apesar de todos os obstáculos, mas também aos colegas e amigos de trabalho, Inês, Tomás, Laura e Diana, que sempre acreditaram que iria conseguir e estiveram sempre disponíveis.

Por fim agradeço ao meu colega Gonçalo, que esteve sempre disponível para me ajudar com todas as dúvidas e questões que fui tendo ao longo do percurso.

Este foi um período não só onde pude ter sucesso a nível profissional como a nível pessoal e estou muito agradecida por todo o apoio e esforço que todos vocês tiveram para que fosse bem sucedida, espero que possa continuar a ter o vosso apoio na minha vida e nas etapas que se seguem e que seja mútuo. Muito Obrigada.

ABSTRACT

Nowadays, companies use consumers' information as a tool to optimize the right offer to the right consumer, but how does the relationship between brand and consumer go when the consumer realizes himself in a vulnerable position? This research aims to understand how brands, in the hotel industry, are endangering themselves by asking customers for their information, by understanding if Data Access Vulnerability has higher downstream effects than control and transparency, without endangering their Brand’s Trust. Two Online Surveys were conducted to understand better the effects of data access vulnerability while doing a booking process. The findings from 160 participants indicate that personal information is a common practice of the industry, having low impacts of vulnerability and are not impacted either by transparency or control. Managerial and theoretical implications are discussed and future research suggestions are provided.

KEYWORDS

Data access vulnerability; Privacy; Trust; Transparency; Control; Hotel industry; Gossip Theory; Communication Privacy Management

INDEX

1. Introduction 1
2. Literature review 4
    2.1. Privacy 4
    2.2. Understanding Vulnerabilities 6
        2.2.1. Data Access Vulnerability 7
        2.2.2. Data Breach Vulnerability 9
        2.2.3. Data Manifest Vulnerability 10
    2.3. Trust 11
    2.4. Transparency and Control 14
3. Methodology 19
4. Results and discussion 20
    4.1. Pretest for Study 1 20
    4.2. Study 1 22
        4.2.1. Participants and Design 22
        4.2.2. Procedure 22
        4.2.3. Measures 22
        4.2.4. Findings 22
        4.2.5. Discussion 25
    4.3. Study 2 26
        4.3.1. Participants and Design 26
        4.3.2. Procedure 26
        4.3.3. Measures 26
        4.3.4. Findings 27
        4.3.5. Discussion 28
5. General Discussion 29
6. Theoretical Contributions 30
7. Managerial Implications 31
8. Limitations and Future Research 32
9. Bibliography 33
10. Appendix 42

LIST OF FIGURES

Figure 1 - Conceptual Model: effect of Customer Access Vulnerability and Suppressors on Trust.. 18
Figure 2 - Distribution of Trust by Brand... 20
Figure 3 - Distribution of Trust by Brand and Gender.. 21

LIST OF TABLES

Table 1- Levene's test 23
Table 2 - ANOVA test description of Trust 23
Table 3 - Descriptive table of Trust 24
Table 4 - ANOVA test description of Transparency and Control 24
Table 5 - Tests of Between-Subjects Effects two-way ANOVA 25
Table 6 - Descriptive table of Transparency and Control 25
Table 7 - Paired Samples Test for Trust Before and After Data Request 27
Table 8 - Descriptive Statistics of Trust Before and After Request 28

1. INTRODUCTION

Marketing professionals began using more targeted methods such as Direct Marketing, and the need for information began to spread with the concept of Databases, turning it into standard practices, by having an interactive approach to individually addressable information (Lock, 1997; Milne, 1999). It became one powerful source to email marketing, providing quick and large ways to contact potential customers with a low cost, bringing to light concerns over personal information (Milne, 1999), and therefore the need for the Permission Marketing concept.

Permission Marketing is a difficult concept to define, according to Godin (1999) consumers can agree to provide their information by opt-in, granting permission in exchange for better targeting of advertising and promotions, reducing the costs of search and vulnerability feeling by building a relationship (Kumar, Zhang & Luo, 2014; Tezinde, Smith, Murphy, 2002; Mishra, Wiley, Gardner, Coughlan, Howell, 2000).

Companies could aim to know better their consumer, according to Forbes, in 2017, 53% of interviewed companies already used big data analytics, which are analytical frameworks that offer approaches to extract knowledge while using machine learning (Suthaharan, 2018). With these practices, companies are trying to optimize more effectively their marketing campaigns with personalized and relevant product offerings, making them the most cost-efficient tools, by turning data collection methods as their main resource to collect information (Martin, Borah & Palmatier, 2017; Martin & Murphy, 2017).

Permission Marketing originated the concept of self-disclosure from a consumers' perspective, being understood as any personal information that a consumer communicates to others. Many of the information that companies use can also be defined as intimate self-disclosure, which is when the information makes them feel vulnerable, either in an emotional/psychological way or in a material way (Moon, 2000). The need for sensitive information in the hotel industry leads to a more vulnerable position by the consumer, by needing ID and credit card information to verify bookings.

In the travel industry, the internet has been one of the most important distribution channels in the last years, because it gives the consumer several benefits that weren't taking into consideration in the traditional travel agents, such as access to more photos, videos, full descriptions, no additional fees and better pricing (Lien, Wen, Huang & Wu, 2015; Letho, Kim & Morrison, 2006; O'Connor & Frew, 2004; Sparks & Browning, 2011).

Businesses are now trying to evolve from Digital to Interactive Marketing, where the consumer is given space to interact directly with the company, with each other and with the media (Kumar, Zhang & Luo, 2014; Winer, 2009), but the consumer still feels vulnerable when providing their personal information (John, Acquisiti & Loewenstein, 2011). Mostly because of the uncertainty of uses given to data but also because of the short-term consequences such as spam emails (John, Acquisiti & Loewenstein, 2011) and the long-term and more dangerous ones, like the occurrence of misused data, hacking and data breaches, where the consumer doesn't know all the ramifications (Martin, Borah & Palmatier, 2017).

Consequently, Consumers' Data Privacy concerns have been rising (John, Acquisiti & Loewenstein, 2011), turning the attention to the imminent potential threats such as vulnerability, fraud, privacy invasion, unwanted marketing communications, highly targeted, obtrusive marketing communications (Martin & Murphy, 2017). Leading into new changes with the laws of GDPR, companies now face the risk of losing millions of euros, if they don't take data protection seriously, according to new laws, already in practice since May 2018, every EU citizen has the right to see his data secured, with more disclosures and opt-in permissions (MarTech Today, 2017).

Although the measures, we argue that these consumers' concerns can still lead to bigger effects in consumer and businesses relationship, by developing vulnerabilities, regarding their personal information, which can damage the consumer's propensity to disclose, their trust and in the long-term the business performance.

As it was shown in previous studies, the suppressors can moderate these negative effects of data access vulnerability in a broader perspective (Martin, Borah & Palmatier, 2017). Using suppressors such as transparency and control, we predict that the impact on trust can be lower depending on the companies' practices and importance given to privacy. What this paper attempts to address is the gap between the effects of suppressors and the Travel Industry, by answering the following question: How can the suppressors moderate the negative impact of Data Access Vulnerability on Brand Trust, in the Hotel Industry?

This research contributes in several manners towards prioritizing the change and improvement of consumers' wellbeing within the travel and tourism industry - something already assumed as an established standard - by demystifying clients' perceived value and vulnerability when supplying their data. It also provides an extension to literature in Travel, more particularly in the Hotel industry regarding data vulnerabilities, focusing on Data Access Vulnerability, with the intent of preparing businesses to face the privacy concerns that affect the day to day (Echeverri & Salomonson, 2019; Anderson & Ostrom, 2015; Anderson, Ostrom & Bitner, 2011).

To support the theory and understand the fully extent of data vulnerability feeling that consumers have, the support of three theories was essential to acknowledge the suppressors, resorting to Gossip Theory, CPM theory and T-form theory.

To test this conceptual model, it was performed two experimental studies, with a series of real case experiments of a booking process while using an online survey, to delineate the effects of the suppressors in the impact of Data Access Vulnerability in Trust while manipulating transparency and control. Following an experimental study to confirm if the Hotel Industry is one with high or low data access vulnerability and consequently the impact of suppressors is conditioned by it.

2. LITERATURE REVIEW

2.1. PRIVACY

Although there is no definition of privacy commonly agreed, because it is difficult to define (Tsai, Egelman, Cranor & Acquisti, 2011; Smith, 1996), there are different perspectives that allow to enlighten the concept and understand better why it is such a concern nowadays.

Privacy can be defined as the condition of being free from being observed or disturbed by other people, according to researchers privacy can be understood as well as the state of limited access to consumer information (Westin, 1967). Being that consumer information privacy can be referred to as related to control of the dissemination and use of the consumer information (Martin & Murphy, 2017; Nill & Aalberts, 2014; Foxman & Kilcoyne, 1993).

There are also different perspectives of privacy around scholars, marketers appear to be using privacy as a strategy because companies can use privacy as competitive leverage. Privacy practices can be a differentiator when consumers' preferences are heterogenous. Although not exploiting customer data when your competitors are can bring companies into a significant disadvantage, privacy measures should be seen as opportunities to improve customers' experience by securing their loyalty. According to a survey conducted by Cisco, in 2019 to over 2601 adults worldwide, 32% of the respondents affirmed that they are willing to act and have done so by switching companies over their data sharing policies, these are known as privacy actives (Redman & Waitman, 2020; Martin & Murphy, 2017).

One of the characteristics that describe these privacy actives, are that although they switch companies based on their privacy policies. They also feel more comfortable with sharing their data in exchange of benefits such as personalized products, being more comfortable with the trade-offs comparing to their non-active counterparts (Redman & Waitman, 2020).

Privacy has become a popular subject among consumers, according to Perrin (2020), 52% of American consumers have decided not to use a product or service because of privacy concerns, among this 52%, 21% decided not to use Websites. This happened because while evaluating the trade-off between the analysis of the risks and benefits of sharing their personal information, meaning while calculating the privacy calculus, consumers were worried about how much personal information would be collected about them. Which can lead to negative word-of-mouth, lower propensity to register online, providing incomplete or false information, opt-out decisions or active complaints (Krafft, Arden & Verhoef, 2017; Lwin, Wirtz & Williams, 2007; Son & Kim, 2008; Sheehan & Hoy, 1999).

The Privacy Calculus, is the concept that clarifies the cognitive process, which presumes a rational thinking, that consumers do, by analyzing the trade-off of their privacy, while contemplating the risks in exchange of receiving a benefit, that can be some kind of utility. This concept has inherent two implicit assumptions, one is that the privacy risks carry some kind of danger, the other is that the consumers are empowered to exercise control over the disclosure (Pomfret, Previte & Coote, L., 2020; Dinev & Hart, 2006; Jiang, Heng & Choi, 2013; Xu, Luo, Carroll, & Rosson, 2011).

Privacy Concerns can be seen as an operationalization of consumers' beliefs, attitudes and perceptions over their privacy (Martin & Murphy, 2017; Malhotra, Kim & Agarwal, 2004; Smith, 1996). Being centred in 4 pillars - collection of personal information, unauthorized secondary use of personal information, errors of personal information, improper access to personal information (Tsai, Egelman, Cranor & Acquisti, 2011; Stewart & Segars, 2012).

In other words and taking into consideration that most of the privacy concerns are related to the online channels, privacy refers to the protection of individually identifiable information on the Internet (Mazurek & Malagocka, 2019). One of the privacy concerns that has been having more heighten is online behavioural targeting which occurs when the consumer detects personalization and obtrusiveness (Martin & Murphy, 2017; Goldfarb & Tucker, 2011).

Concerning online privacy, it is mandatory to understand the dimensions that feature it. In Online Privacy, the dimensions observed were awareness, that refers to the knowledge of the data that is being transferred can be used in the future with risks, collection which refers to the ethical and legal regulations that control and analyze the collection of data, and control, considered one of the main factors by scholars, that regards the power that the consumer has over their information (Mazurek & Malagocka, 2019). Most consumers' would appreciate having more control, more specifically over how their information is used, which would alleviate their privacy concerns (Phelps, Nowak & Ferrell, 2000).

Although there are privacy concerns among consumers, and they have gained much notoriety and concern to the companies, consumers tend to not change their behaviours, meaning that consumers tend to share their information while being concerned, which brings to light the concept of Privacy Paradox. Privacy Paradox is the relationship that occurs between individuals' intentions to disclose personal information, through surveys for example and the actual behaviours to disclose (Pomfret, Previte & Coote, 2020; Martin, 2019; Barth & Jong, 2017; Martin & Murphy, 2017; Aguirre, Mahr, Grewel, Ruyter & Wetzels, 2015). They tend to have this behaviour while acknowledging the risks of sharing their information in exchange of value and personalized services (Barth & Jong, 2017).

Inside the privacy paradox, although there isn't any widespread cross-disciplinary acceptance, there are different arguments that can be analyzed to understand better the concept. The strongest one, the No-Privacy-Exists, summarizes that the consumers' privacy doesn't exist at all, because while visiting a website or an app, the consumer relinquishes their privacy expectations. This argument defends that the privacy is defined as a complete state of isolation (Martin, 2019; Barth & Jong, 2017). According to this argument, companies have no responsibility to understand or meet consumer privacy expectations. The other argument represents a weak privacy paradox, where Privacy-Can-Be-Traded implies that consumers' may have reasonable privacy expectations but still demonstrate their willingness to trade the risk of disclosure for the benefits that companies might offer, meaning that the privacy calculus leads to a disclosure of information. According to this weak privacy paradox argument, companies can do what they wish with the consumers' personal information , as long as they collect it without fraud or deception. At last, the no paradox argument, states that there is a consistent behaviour of the consumers, meaning that as they state the concerns and expectations that they have with privacy, consumers retain all this after engaging with firms, still expecting that firms respect the norms of privacy. Taking into account this argument, privacy is described as a core value necessity to individual development but also to build intimacy and relationships, while flourishing societies (Martin, 2019; Cohen, 2012; Nissenbaum, 2010; Regan, 1995).

The privacy paradox behaviour, creates an effect on firms, that makes them have little to no responsibility to identify or respect for consumers' privacy expectations (Martin, 2019).

When the consumers' privacy expectations don't match the company actions, the perceived privacy violation, meaning the perception of control that consumers has over when, how and what is being communicated to others about them can have negative effects on companies. Privacy Violation can go from Severe Privacy Violation, where the privacy expectations compared to company actions don't match at all to Minor/ No privacy Violation, where the alignment of both variables are almost equal (Wright & Xie, 2017; Pollach, 2005).

2.2. Understanding Vulnerabilities

To better understand the phenomenon behind the process of data collection and the implication it has on the consumer it's needed to understand which ramifications the vulnerability feeling has.

A vulnerability is understood as susceptibility to injury or harm (Smith & Cooper-Martin, 1997), which causes the consumer to be anxious regarding the potential damage/violation in this specific case applied to their personal data (Janakiraman, Lim & Rishika, 2018; Martin, Borah & Palmatier 2017; Scharf, 2007).

To be able to understand Vulnerability, researchers have to listen or observe the experiences that the consumer has. By perceiving vulnerability others have to believe that a person is vulnerable, independently of the own person's perception (Baker, Gentry & Rittenburg, 2005).

Consumer Vulnerability can be seen as the state of powerlessness that comes from an imbalance in the marketplace interactions or from the consumption of marketing messages and products. It occurs when control is not in an individual's hands and can be observed by analyzing consumers' experiences. It arises from the interaction of individual states such as mood and transitions, individual characteristics like psychological and biophysical, and external conditions for example physical elements, in a more specific context such as a purchase (Echeverri & Salomonson, 2019; Baker, Gentry & Rittenburg, 2005; Moschis, 1992).

Taking Consumer Vulnerability to the spectrum of Data and Privacy concerns, the feeling of data vulnerability is a particular one, because it refers to all the collection, storage and use of personal information that companies do and that creates the feeling of potential harm in the consumers. There are 3 types of data vulnerabilities: Data Access Vulnerability, Data Breach Vulnerability and Data Manifest Vulnerability, which occur in a continuum potential of harm, across different stages and interactions between the consumer and the company, and have different implications for the consumer online security and feelings (Martin, Borah & Palmatier, 2017).

2.2.1. Data Access Vulnerability

Data Access Vulnerability is the most benign form of data vulnerability, but also can be the first step of interaction between consumer and brand. Here lays the opportunity to get to know the consumer and to develop a relationship, this occurs when the consumer is asked for his information and afterwards, the company has the possibility to store and use it (Martin, Borah & Palmatier, 2017). It can happen many times on our day, for example when we subscribe to a newsletter, when we fill a form to get a promotion voucher, or even when we register in some website to be able to book an hotel.

To prevent and reduce feeling vulnerable, the customers' limit how and whom they share sensitive information (Martin, Borah & Palmatier, 2017), by limiting self-disclosure. This can be seen as an act of reactance, which is a motivational state in which consumers resist a phenomenon by acting in the opposite way to what is intended (Tucker, 2014; Brehm, 1989; Clee & Wicklund, 1980). Self-disclosure is an important action to understand the data access vulnerability variable and the implications it has on the mind of the consumer. It is stated as any personal information that a person communicates to another (Moon, 2000). Some examples of intimate self-disclosure are Name, ID number, Credit Card Information which are types of information that usually are collected by any Hotel Company to verify the authenticity of the booking.

Different variables can highly influence the relationship between the owner of the information and the “authorized co-owners”, in this case, the companies in terms of self-disclosure. These variables can be ones such as brand equity, previous relationship, income, gender and others, but more relevant for this study the type of sensitivity that the information conceals and the trust that consumers have in the brand, previous to disclose their information.

The type of data and the sensitivity that the information has can be one of the most relevant concerns that companies face when dealing with self-disclosure. Consumers can indicate what type of information they feel it is sensitive and withhold it. Individuals that start a purchase flow, may pay attention and analyze the adequacy or relevance of the data requested. For example in the case of a hotel booking asking for personal information such as credit card number and identifiable information such as name, can be seen a more reasonable request than asking for hotel preferences, which can be seen and predicted as invasive communications (Mazurek & Malagocka, 2019).

Another important conditioning to self-disclosure is the appearance of the website, which can raise red flags, therefore it is important that companies work on having a professional appearance and avoiding similarities to websites related to phishing and fraud (Mazurek & Malagocka, 2019; Conti & Sobiesk, 2010). Besides this, it is important for companies to not abuse on the personalization of their advertisements, with the risk of being perceived as invasive and leads the consumer to react negatively towards personalized communications, making them see as intrusive (Mazurek & Malagocka, 2019; Krafft, Arden & Verhoef, 2017; Goldfarb & Tucker, 2011).

In a chance to relieve the pressure caused by self-disclosure while being target to advertisements or while the booking process, is that consumers tend to react better to the variable of Reciprocity Appeal arguments compared to Relevance arguments. Relevance arguments, are one of the dominant strategies used by marketeers, which highlight the offer of relevance in advertising in return of consumers’ personal information (Schumann, Wangenheim & Groene, 2014). Opposite to the relevance appeals, reciprocity Appeal Arguments appeals emphasize a social exchange for free services, this can be applied to an exchange of information in return to benefits, such as promotions and incentives instead of Relevance argument based on increasing relevance to the consumer. It is believed that Reciprocity Appeals may be one of the essential reasons why individuals are willing to share their private information and why the concerns regarding privacy don't translate into higher conservative behaviours, since reciprocity appeals motivate people to reciprocate, because of social norms, positive self-image and other's view of them (Mazurek, G., Malagocka, K.,2019; Schumann, Wangenheim & Groene, 2014; Alpizar, Carlson & Johansson-Stenman, 2008).

Another theory associated with the disclosure of personal information and that studies the relieve of pressure in it, is the Communication Privacy Management, known as CPM. This theory is related to the process of managing to disclose and protect private information. CPM Theory admits that the individuals believe their private information is owned by them and they have the right to control it. By owning their private information, the theory accepts that the consumers form metaphoric boundaries of where people store and protect their information. When the possibility of sharing their information, individuals have a mental calculus, known also as privacy calculus, where they can decide to share or to keep their personal information (Pomfret, Previte & Coote, 2020; Petronio, 2002). Meaning that there is a preconception that people believe they have control and trust that they can grant access to their private information to whom they want and their limits to it (Petronio,S. & Child, J., 2020).

The perception of Vulnerability will likely diminish the willingness to disclosure and to help companies avoid the impact that Data Vulnerabilities can have on themselves. The combination of transparency and control, can generate a feeling of empowerment, even if their vulnerability is significant (Baker, Gentry & Rittenburg, 2005), combined with the Reciprocity Theory that leads to higher acceptance of advertising (Schumann, Wangenheim & Groene, 2014), can help with suppressing the negative effects of vulnerability and influence the ability to self-disclose.

In the Hotel Industry, disclosing personal information is inevitable when making an online hotel reservation (Lee, Au & Law, 2012), which can lead to a higher Data Access Vulnerability because it is usually an intimate self-disclose type of information which means that it is perceived as high-risk information that creates the feeling of vulnerability (Moon, 2000), such as contact information and credit card number, which triggers customers' privacy concerns (Lee, Au & Law, 2012).

2.2.2. Data Breach Vulnerability

Data Breach Vulnerability is probably the most known type of data vulnerability, not only because it can have more negative effects but also because they are highlighted regularly in news' headlines (Choi, Johnson & Lehmann, 2019). It occurs when a security lapse is detected where the lack of control and the unknown makes the consumer feel anxious, since the unauthorized individual has access to it, but the consumer doesn't know if the data will be used or sold to other entities. This security violation involves sensitive, confidential or protected data (Richardson, Smith & Watson, 2019; Privacy Rights Clearinghouse, 2018; Martin, Borah & Palmatier, 2017). One of the most advertised breaches in Hotel Industry was the Marriott Hotels breach, where hackers had compromised their customers' information, around 500 million guests had their information breached, which still has effects nowadays because guests still don't know exactly what happened, how the hackers entered the system and the final consequences of this breach. The information accessed were names, email addresses, phone numbers, passport numbers, passwords, some of the guests' credit card information and other types of personal information. (Lee, H., et. al, 2012; Simon, M., 2019). Although not every consumer is victimized by this security lapse, the perceived threat and the uncertainty leads to higher levels of vulnerability (Palmatier & Martin, 2019).

When Data Breaches occurs, companies also have tangible and intangible costs such as legal counsel, loss of reputation, class action settlements, intellectual property, exposing operational control risks and showing the need to improve computer systems (Richardson, Smith & Watson, 2019; Layton and Watters, 2014; Gwebu, Wang, and Xie, 2014; Morgan, 2017; Lawrence, Minutti-Meza, and Vyas, 2018).

Apart from the concerns that on a Data Breach Vulnerability the company has its own records breached, there are also concerns regarding the delays to public disclosure (Cheng, X. & Walton, S., 2019; Tsukayama, 2017). The Data Breach Announcements Besides that, the company can also suffer from other companies data breaches, this effect, known as spillover effects, occurs when a similar firm has a data breach which leads the consumer to feel vulnerable and perceive a bigger susceptibility to harm because of it. Usually this similar firm can be a competitor and although it has its effects it can has lower vulnerability than the company having their own breach (Palmatier & Martin, 2019; Martin, Borah & Palmatier, 2017).

2.2.3. Data Manifest Vulnerability

Data Manifest Vulnerability is when the data is misused, harming the customer. This makes the consumer feel violated and unable to see the extension of the threat (Anderson, 2013) It can happen in many forms, the data can be sold, targeted by other companies or it can end in identity theft, depending on the sensitivity of the data.

With the rise of data vulnerabilities caused by everyday communication, the concern for privacy arises, leading to some consumers to even attempt to block marketers efforts to reach them with Ad Blockers, Spam Emails, and faking the information they give. Although Data Privacy, is a difficult subject to define, because of its different perspectives and ramifications, Data Privacy in Marketing has been used as strategic leverage, with the goal to increase acceptance and willingness to disclose information, by securing loyalty and positive brand experience (Martin, 2017).

There has been an effort to return the privacy to the consumers, since May 2018, European Laws on Data Privacy, General Data Protection Regulation or known as GDPR, are forcing companies to give more control to consumers regarding their information, impeding the dissemination of personalized and individualized marketing practices. According to Momen, Hatamian & Fritsch, 2019 on "Did App Privacy Improve After the GDPR" the GDPR laws are expected to create more protection regarding personal data, increased transparency of collection and processing and stronger intervention rights of data subjects. These laws already applied sanctions to big companies such as Google, that has been fined in 50 million euros, for not giving enough information to its user and having lack of transparency regarding their policies of consenting shared data, according to BBC News. Since the implementation of GDPR in May 2018 is estimated that there was an overall of $126 million in fines, according to CNBC.

Besides the data vulnerabilities and due to the phenomenons regarding the evolution to interactive marketing and in technology, there is also a specific effect named customer vulnerability escalation. The effect is created by the AI increase in companies, which allowed to alienate customer groups, focuses on reaching more profitable customers and created an exclusion of customers that can be seen as discriminatory (Palmatier & Martin, 2019).

2.3. TRUST

Customers start the booking process with a certain level of trust and their goal is to make a good deal, meaning that both, company and consumer are looking to a win-win relationship (Mazurek & Malagocka, 2019). To guarantee that the consumer doesn't see their trust affected while purchasing, it is important to mitigate the vulnerability feeling.

In a more broad perspective, Trust is understood as the willingness to rely on an exchange partner in whom one has confidence, believing in the competence of another to perform a specific task, meaning that trust is divided by both behavioral and cognitive aspects (Schlosser, White & Lloyd, 2006; Moorman, Deshpandé & Zaltman, 1993). Furthermore, Trust is one of the most significant factors to develop social relationships, and for it to be higher both parties need to have coincide expectations and the best interest of each other independently of their own personal expectations (Izogo, Jayawardhena & Adegbola, 2018; Simpson, 2007; Morgan & Hunt, 1994). It can also be described as the acceptance of vulnerability that it might offer to the person (Etzioni, 2017; Bart, Shankar, Sultan & Urban, 2005).

By Cognitive and Behavioral aspects we take into consideration the Trusting Beliefs and Trusting Intentions, which have focal presence to exist Trust. Trust can be originated from different cognitive processes applied to persons and institutions that are considered trustworthy, distrustful or unknown (Yeon, Parka & Lee, 2019; Lewis and Weigert, 1985). This cognitive processes are known as Trusting Beliefs, which can be separated into three dimensions: Ability, Benevolence and Integrity beliefs.

Ability beliefs refers to the skills that a company can perform, meaning that the consumer will believe that certain company can do what it has promised, Benevolence beliefs refers to the company's positive orientation, believing that the company besides having the profit motive has a positive orientation towards the consumer and wants to add value to them and at last, Integrity beliefs, are referring to the moral principles that a company has, by following the code of professional standards (Schlosser, White & Lloyd, 2006; Mayer, Davis & Schoorman, 1995).

Concerning Trusting Intentions, it focuses on the willingness of making oneself vulnerable, while in presence of risk, by being the main difference between behavioral beliefs, the risk and the perception of it existing (Schlosser, White & Lloyd, 2006; Moorman, Deshpandé & Zaltman, 1993).

According to Mayer, Davis and Schoorman (1995) Trust is a subjective interpretation and to understand it , three approaches can be followed. First, propensity theory, relies on individual characteristics, based on how an individual intends to trust. Second, behavioral decision, that claims that trust is a rational decision-making process where the centre is immediate situational factors. Third, the institutional approach, that claims that trust can be influenced by situational factors and organizational an institutional structures.

In a commerce perspective, Trust can also be deconstructed into a multidimensional feature formed by Cognitive Trust and Emotional Trust. Cognitive Trust includes dimensions of integrity, which refers to the willingness to keep promises, benevolence that involves generous behavior that leads to wellbeing of consumers and ability, which is regarding the capacity of having consumers. It is formulated by the accumulated knowledge that the consumer has regarding the company (Kim & Kim, 2019; Yeon, Parka & Lee, 2019; Johnson and Grayson, 2005). Emotional Trust is created through the relationship that a company has with the consumers, meaning how the consumer feels about a company (Yeon, Parka & Lee, 2019).

The concept of Trust can be divided into multiple other concepts, such as Online Trust which are the consumer perceptions related to the website, internet and technology, of how it might deliver face to the expectations, how believable the information might be and the confidence it transmits (Bart, Shankar, Sultan & Urban, 2005). Online Trust differs from the Offline Trust, that is based on a storefront and can't be replicable, since the cues aren't present on online settings and aren't so easily interpreted (Etzioni, 2017; Bart, Shankar, Sultan & Urban, 2005). The Online Trust relies on the appearance of the website and the sense of security that it perceives to the consumer, some of the signals used to help with online trust is the incorporation of seals of approval by third parties (Bauman & Bachmann, 2017).

In Online Trust there are certain risks that are perceived more damaging than others depending on the category and industry of the company, in the Travel industry the information risk is the underlying website factor that has presence, meaning that there is an uncertainty associated with providing personal information that could be exposed (Bart, Shankar, Sultan & Urban, 2005). There are some determinants of online trust, such as personal characteristics, website features, system structural assurance and specific consumer cultural characteristics (Bauman & Bachmann, 2017). Besides the most influential determinants for Online Trust to happen in Travel websites, are Privacy, which can be understood as the protection of individually identifiable information involving the implementation of a privacy policy, notice, disclosure and consent of the Web site visitors, and order fulfillment that refers to the ability to deliver every product/service that were requested by consumers (Bart, Shankar, Sultan & Urban, 2005).

Furthermore, the site isn't the only method to confer trust, travelers are increasingly dependent on online reviews, trusting them for travel planning, meaning that if consumers perceive authenticity of online reviews, their trust will be bigger (Kim & Kim, 2019; Lee, Au & Law, 2012) since online Reviews tend to form online trust, the reviews must be a source of credibility, which is a measurement of the level of truth and validity of received messages (Hsieh & Li, 2020).

Taking into consideration the transmission of data from clients to the company, meaning the process of Data Access Vulnerability, it is important to focus on the different dimensions that trust has. According to the T form theory, there can be two types of trust. Trust in the Brand, which as it implies, trusting in the service or product that the brand offers, which can be perceived as an offer with implied benefits , meaning that to have access to the service you disclose, or as the value, where the consumer perceives as a benefit to disclose, gaining additional value, such as more tailored ads, special discounts, and others (Mazurek, G. & Malagocka, K.,2019). Consumer trust and satisfaction with the transaction will also affect the possibility of forming a long-term commercial relationship between a company and a customer (Bauman & Bachmann, 2017; Kim, Ferrin, & Rao, 2009; Morgan & Hunt, 1994).

2.4. TRANSPARENCY AND CONTROL

The e-commerce reality is that companies collect personal information and compile it in ways that consumers had not envisioned it, this act has been increasing more and more in an era of technology. Which brings to the consumer feelings of vulnerability (Martin, Borah & Palmatier, 2017; Tucker, 2014), that more likely can lead to consumers feeling violated and lose trust in a company (Palmatier & Martin, 2019).

Data Access Vulnerability might have lower effects than other forms of data access vulnerability, by giving the possibility to companies of having a "detailed digital dossiers about consumers." (Palmatier & Martin, 2019) but with the feeling of Vulnerability spread into the mind of the consumers, the data vulnerabilities, the concerns for privacy rising and the urge to protect the consumers' trust, the need to find answers and to develop new strategies to mitigate the negative effects rose and although the theoretical marketing already has the knowledge that all types of data vulnerability come with significant negative effects, not only to the company who suffers from the effect but also the competitors due to spillover effect (Martin, Borah & Palmatier, 2017), the need to mitigate the negative effects lead researchers to try and find solutions which brought to light some useful theories that discuss new variables which companies can use to prevent the vulnerability feeling to spread inside the consumer and incentive the process of self-disclosure.

Furthermore, the available studies nowadays don't focus either on such a specific industry like Hospitality or on a more deep analysis of data access vulnerability. It is important to extend the knowledge of data access vulnerabilities, because it is the first step into the privacy concerns that consumers might have and to the feeling of vulnerability, which might influence trust as it is important to measure what are the implications to the feeling in the hotel industry and if it can be suppressed.

These negative effects can be suppressed by a couple of variables, variables that are commonly known as the suppressors according to the Gossip Theory and are approached also by other theories, that take into consideration different inputs and different perspectives converging into the Customer Control and the Transparency that a company shows and gives to the consumer. It will work in a way to help the vulnerability feeling to spread inside the consumer and avoid the consumer to perceive an online transaction risk by Empowering him and leading to an higher trust in the company (Martin, Borah & Palmatier, 2017; Baker, Gentry & Rittenburg, 2005).

To understand better the use of suppressors, first we have to understand the theories behind them, in a more specific case the Gossip Theory, the CPM theory and the T form theory.

The Gossip Theory refers to the feelings regarding vulnerability that the consumers' psychological and behavioral responses have. It also suggests that in a business context, data vulnerabilities may lead to emotional violation and lowered evaluations of trust (Martin, Borah & Palmatier, 2017). According to Gossip Theory there are two factors that can suppress the negative effects of powerless transmissions of information - transparency and control. Transparency refers to the awareness and the details about which information is being shared. Taking into the process of booking a hotel, this means being aware that the Hotel is collecting information such as the credit card number and that this information is being collected to process the payment. Control is associated with the perception of managing the flow of information, consumers can perceive the lack of power that they have in containing where the information goes or how is it used (Martin, Borah & Palmatier, 2017; Emler, 1994).

According to CPM, the variable of Control is the essence of tempering feelings of susceptibility, by the individuals having control of their personal information. This Control is related to having control to their Privacy Boundaries, which is one of the bases of the CPM theory. These are related to where people store and protect their information (Petronio & Child, 2020; Petronio & Gaff, 2010). Adjusting the CPM to the relationship between consumers and companies, consumers have Control by having control of their boundaries, meaning the ability to disclose their information to a certain company or not. The Control from the CPM theory is understood as one of the simpler ways of having control regarding your personal data.

The T-form theory, analyzes the ways to succeed in transferring data from clients to the company, which means the process of self-disclosure, that may lead into Data Access Vulnerability. This theory claims that in order to have this process being successful companies depend on the three Ts, working on a closed system and that have factors influencing their success individually, allowing the customer to not be made uncomfortable (Mazurek & Malagocka, 2019). The three T's are transparency, type of data and trust, regarding Transparency, it will help dealing with data collection and communication, allowing a clarification of how the the procedures of data collection and communication work and how the third parties are involved and have access to data transferal. The Type of Data involves the perception that personal information has, and if while being asked the consumer has a perception that the request is adequate and relevant for the company, which can be related to one of the pillars of GDPR. The data focus, where the data that is requested is needed to perform advertising (Mazurek & Malagocka, 2019; Schweigert & Geyer-Schulz, 2019). And the last T is Trust, trust as analyzed prior in this research, can be comprehended as the acceptance of vulnerability that it might offer to the person (Etzioni, 2017; Bart, Shankar, Sultan & Urban, 2005), here trust is relevant because it reduces the perceived risk of entering into a transaction and can increase the chances of market success, by understanding the value that they get by revealing information (Mazurek & Malagocka, 2019).

Taking into account the theories, we can summarize both this variables, in one hand, Transparency is when companies provide information about how they collect, share and protect data (Martin, Borah & Palmatier, 2017). It should explain why the company needs the customer data, and what purpose it has to do with it. In more detail it can be their privacy policies, the type of data they collect, how do companies use data after collecting and how can that process impact the consumer, clarification regarding third parties should be mentioned (Mazurek & Malagocka, 2019).

This action can prevent the feeling of vulnerability to spread by informing the consumer and it can be a critical vulnerability suppressor because it gives the consumer the knowledge that allows him to evaluate the potential harm that might come by giving access to their personal information (Palmatier & Martin, 2019). Not only Transparency is an important factor from Literature theories and a recommended best practice, but is also an important factor demanded by GDPR law (Mazurek & Malagocka, 2019).

Knowing this, since it has been implemented as a best practice, is demanded by the GDPR law and has been proved that Transparency can suppress the negative feelings of gossip (Martin, Borah & Palmatier, 2017; Beersma and Van Kleef, 2012), we propose that Transparency can mitigate the feeling of data access vulnerability and the negative effects that is has on Trust on a hotel company, reducing the negative feeling or turning it into a nule effect.

H1: The negative effect of Data Access Vulnerability on Trust is reduced by Transparency.

In one hand, Customer Control are the means to empower the customers regarding their data, giving the option to choose what data they can disclose and data management decisions, such as opt-in and opt-out from Databases. Although only 49% of consumers know about this, control is an important part of privacy protection, even being part of its definition. Privacy can be understood as having control over personal information flows (Brandimarte, Acquisti & Loewenstein, 2012; Kang, 1998; Solove, 2006; Tavani & Moor,2001). Control can be addressed as two perspectives - over disclosure and over usage.

Control over disclosure is more related to the Data Access Vulnerability, where users can choose every detail of the information that will be available and choose who knows it. It can go from a high level control personalisation like in Social Media or it can be only choosing if a certain company can have access to my information (Brandimarte, Acquisti, Loewenstein, 2012).

Control over usage, is related to the third-parties, that can be partners of the entity to whom we disclosed, that can have access over the information and use it for their purposes. Usually this type of practice can be only understood by the consumer when receiving intrusive communications, targeted advertising or price discrimination (Brandimarte, Acquisti & Loewenstein, 2012; Acquisiti & Varian, 2005).

Transposing to Gossip Theory, often the targets try to regain control over their information, being a restorative element after a damaging gossip event, but also it can prevent the damage feeling of data access vulnerability, because while having control over their personal information, customers can choose to opt-out at any time or manage their privacy preferences (Palmatier & Martin, 2019), by being empowered over it, the consumers' feeling of vulnerability can be suppressed on Trust will more likely to be reduced or be equal to 0.

H2: The negative effect of Data Access Vulnerability on Trust is reduced by Control.

Taking into account, all the theories that approach the reduction of vulnerability feeling and to be able to suppress the feeling of vulnerability almost completely, it is needed to integrate all theories and rely on both Transparency and Control, bearing in mind that if companies have low both on transparency and control, meaning that consumers can have any the feeling of vulnerability without any mitigation of it, this will be the highest negative feelings that the consumer can have, which we call the neutral stage of this analysis (Martin, Borah & Palmatier, 2017).

While having high transparency and low or none control, it means that the company will be complying with the best practice from the GDPR law, the consumer might perceive more the risks of violation and lower trust, specially in cases where the data vulnerability is higher, since this will give the knowledge that the data is being collected and the procedures it suffers, but the means of acting about it are not given (Palmatier & Martin, 2019; Martin, Borah & Palmatier, 2017).

When the consumer has transparency deficit and high control, the consumer will have the ability to make an uninformed choice, by not having the fully knowledge of the process of data privacy, leading to a more difficult process of decision (Palmatier & Martin, 2019; Martin, Borah & Palmatier, 2017).

Meaning that to achieve the most empowering proposition, the consumer will have both high elements of transparency and control, the consumer will have fully knowledge of what his data might be used and how he can control and manage his privacy settings and even opt-out after opting-in, knowing that he has choices (Palmatier & Martin, 2019; Martin, Borah & Palmatier, 2017; Baker, Gentry & Rittenburg, 2005).

H3: The negative effect of Data Access Vulnerability on Trust is reduced by the interaction between Transparency and Control.

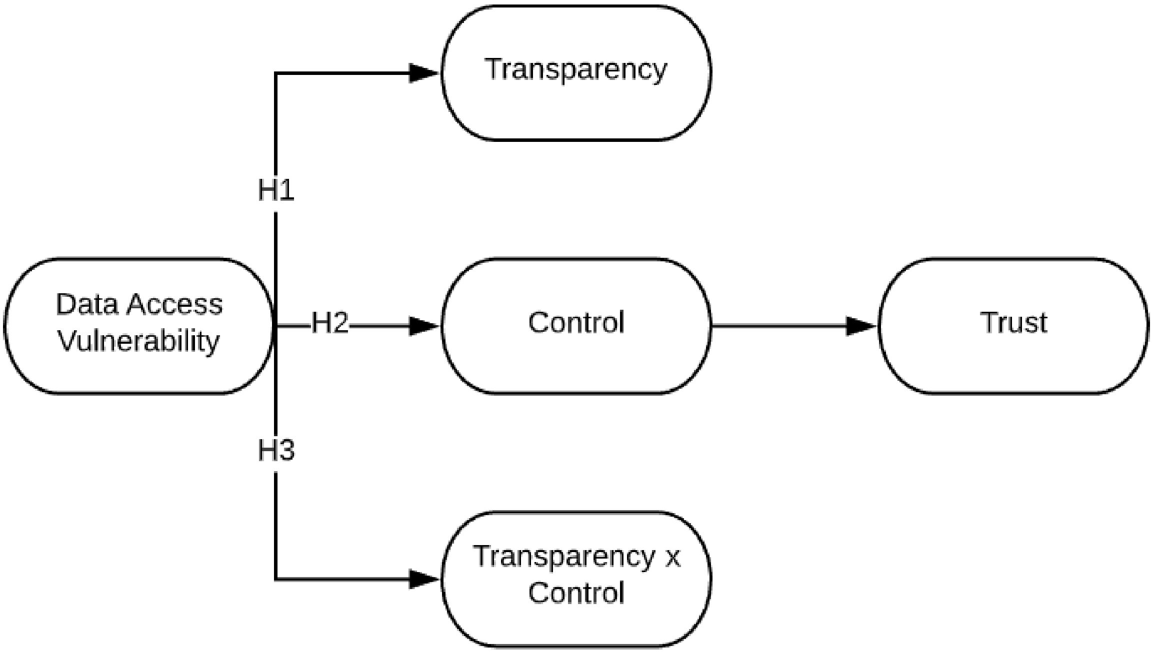


Figure 1 - Conceptual Model: effect of Customer Access Vulnerability and Suppressors on Trust

3. METHODOLOGY

Both experiments were conducted by quantitative methods, through online questionnaires with the intent of testing our prediction on how suppressors can affect Trust while being exposed to a situation of Data Access Vulnerability, in the Hotel industry.

Since this is a vulnerability that comes through the request of information and to be perceived has to be observed as a potential danger and also because the privacy paradox effect shouldn't affect the answers, the need to be able to insert the respondent on a real-life scenario was mandatory. To do so and to be able to test this condition, we conducted a pretest with a goal to understand which Brand would be the one that would generate less bias in the mind of the consumers because of the pre-condition of trust that brands can have, which is one relevant variable of the T-form theory and would mitigate the results (Mazurek & Malagocka, 2019).

In Study 1 we resorted to an online survey, that was described as a real-life scenario of a booking process, leading to an analysis and comparison of the answers of one hundred and sixty respondents between four groups of people that would be randomly assigned to each hypothesis request. The hypotheses were individually analysed and compared throughout the groups, to understand the suppressing effects of the variables Transparency (H1), Control (H2) and the combination of both (H3) on Data Access Vulnerability relationship with Trust.

Our Study 2 provided evidence to support and justify the results behind Study 1, following the same model as the previous study. By being exposed to the suppressors the mitigation effect on the negative impact of Data Access Vulnerability on Trust didn't occur, because of the not significant existence of Data Access Vulnerability effect on Trust. This study in the quantitative method offered the possibility to compare only Trust before and after the request for their information.

All the online surveys were filled anonymously, and their responses were only used to the purpose of this study, to be able to protect the respondents and maintain their privacy safety.

4. RESULTS AND DISCUSSION

4.1. PRETEST FOR STUDY 1

Before conducting Study 1, we tested perceptions regarding the level of Trust of different Travel Brands, including both Hotel Chains and Booking Platforms, with an Online Survey with 30 participants. (43,3% percent women, M_{age}=33)

The goal with the pretest was to choose what brand would have a more moderate level of Trust, since that usually Trust increases the tendency towards openness and disclosing between company and possible clients. So to be able to not have any bias, the brand chosen was the one with a more Moderate Level of Trust (Mazurek & Malagocka, 2019).

Participants categorized 13 brands with the level of trust that they have in each one.

As shown on Figure 2, which demonstrates the list of Brands that were evaluated by the respondents, They were Pestana Hotel Group (M_{Trust} 8.43), Vila Galé (M_{Trust} =7.22), Tivoli Hotels (M_{Trust} =7.30), Booking.com (M_{Trust} =7.04), Momondo (M_{Trust} =3.91), AirBnb (M_{Trust} =5.17), Expedia (M_{Trust}=4.43), HomeToGo (M_{Trust} =2.57), Accor Hotels (M_{Trust} =5.57), Hoti Hotels / Meliá Hotels & Resorts (M_{Trust} =6.43), Marriott Hotels & Resorts (M_{Trust} =7.74), Minor Hotels (M_{Trust} =3.78), Sana Hotels (M_{Trust}=6.91).

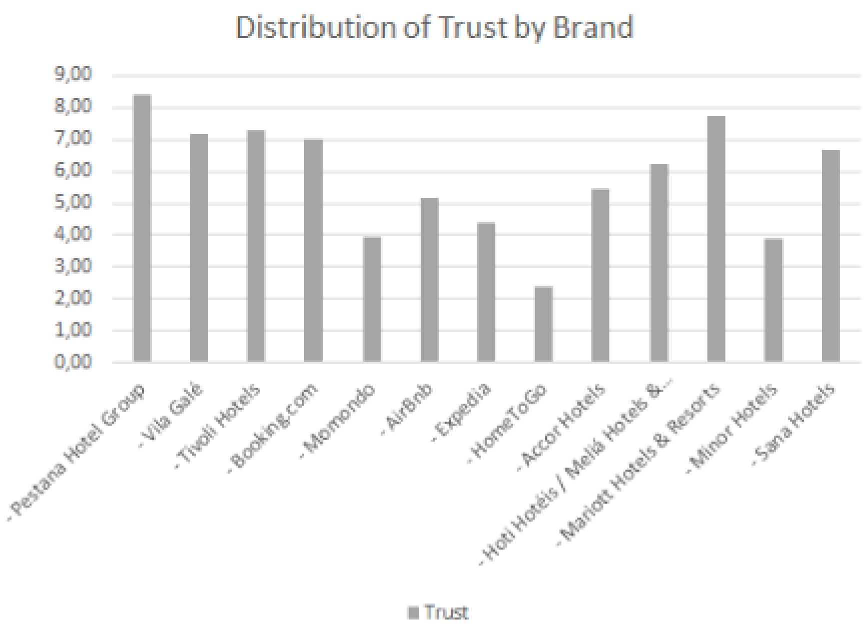


Figure 2 - Distribution of Trust by Brand

Analyzing the behaviour per gender, the respondents classified the brand with an average level of M_{Trust} =5.45 for Female and M_{Trust} =6.13 for Male, showing in a broad perspective that Male have more trust in brands, although per brand the behaviour was different.

As represented on Figure 3 ,the brand with highest ranking of Trust in this analysis, on Females was both Pestana Hotel Group with M_{Trust} =8.08 and Marriott Hotels & Resorts, with an M_{Trust}= 8 rating. For Male, it was Pestana Hotel Group with M_{Trust} =8.71, followed by Marriott Hotels & Resorts with M_{Trust} =7.59.

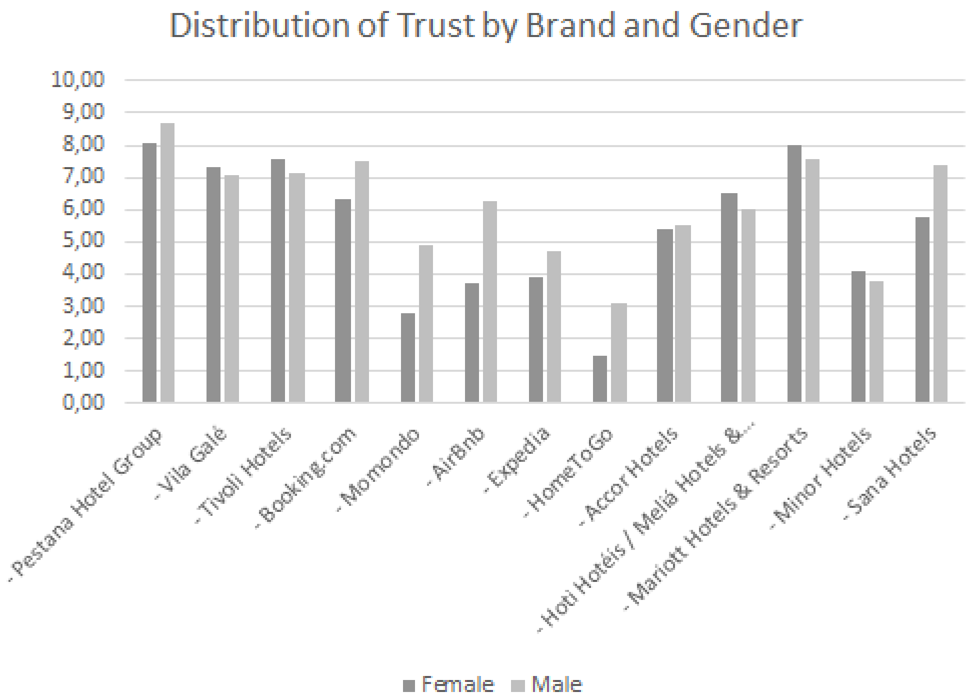


Figure 3 - Distribution of Trust by Brand and Gender

Overall the brand with the average value most close to the average M_{Trust} =5 , was AirBnb with M_{Trust} =5.17. Since the goal of the dissertation is to evaluate the specific behaviour of the request in Hotel Brands, the Brand chosen was Accor Hotels, with an average of 5.57 of Trust. The lowest level of Trust is shown in the HomeToGo, with M_{Trust} 2.40, which could indicate not only the lack of trust in this brand but also the lack of knowledge about it.

4.2. STUDY 1

4.2.1. Participants and Design

One hundred and sixty respondents voluntarily participated in a scenario-based experiment (66,9% percent women), where the participants were randomly assigned to each case (*n*=40) having the context of booking a room for Accor Hotels.

4.2.2. Procedure

Participants were asked to imagine a scenario where they were booking a room in Accor Hotels' Official Website and were asked to release information, such as Name, Country, Phone Number, Email and Credit Card Number as part of the reservation process adapted from other researches (Lee, Au & Law, 2012; Martin, Borah & Palmatier, 2017).

Later each participant was randomly assigned to test one of the conditions of the hypothesis, in which they were divided into four groups to test the hypothesis: Control Group, Privacy Control, Privacy Transparency and Privacy Control x Privacy Transparency.

To develop the most realistic case as possible, we first collected copies of privacy policy statements from real hotel chains' websites and adapted it from Martin, Borah & Palmatier, 2017 making sure that it complied with a understandable message, free of specific legal/technological references, while maintaining a friendly and straightforward language (Mazurek & Malagocka, 2019).

4.2.3. Measures

Trust is the main dependent variable in Study 1. Participants indicated their level of Cognitive Trust by answering to 4 questions: "I trust Accor Group", "Accor Group is very trustworthy", "I have confidence in the Accor Group's behaviours", "Accor Group is reliable" Answers were coded from 1 (strongly disagree) to 7 (strongly agree) scale, adapted from Martin, Borah & Palmatier (2017).

After this rating, participants were asked for demographic information which included age, gender and level of education. Finally, participants were asked to rate the level of Transparency and Control that they have perceived in the scenario experienced.

4.2.4. Findings

Participants were asked to classify the level of Trust after experiencing booking a room at Accor Hotels' Website. To be able to test the scenarios and see if there is any difference between samples, the test to analyze the variance or one-way ANOVA needs to fill 3 assumptions.

The first is that the samples are independent, which is true since the three samples were different subjects without any relation. The second is that the samples are taken from a population with normal distribution, which is assumed since the samples are bigger than 25 and the third and final assumption is the homogeneity of variances which can be tested by Levene's test.

		Estatística de Levene	df1	df2	Sig.
Trust	Com base em média	2,193	3	156	0,091
	Com base em mediana	2,049	3	156	0,109
	Com base em mediana e com gl ajustado	2,049	3	140,588	0,110
	Com base em média aparada	2,209	3	156	0,089

Table 1- Levene's test

Looking to the Levene's test, in Table 1 we can acknowledge that the homogeneity of the samples is guaranteed, meaning that the $F_{(3,156)}$=2.193; p=0.091; since p>0.05.

Proceeding to test the ANOVA, Table 2 displays the studies, where we tested the 4 scenarios, in which we found none significant effect between the request of information (Data Access Vulnerability) and the level of Trust in a Hotel chain brand, while being present with the suppressors. $F_{(3,156)}$= 1.139; p= 0.335; $\eta p2$= 2.502, since the p= 0.335 < 0.05. Which indicates that the suppressors didn't have the effect expected.

		Soma dos Quadrados	df	Quadrado Médio	Z	Sig.
Trust	Entre Grupos	7,506	3	2,502	1,139	0,336
	Nos grupos	342,563	156	2,196		
	Total	350,069	159			

Table 2 - ANOVA test description of Trust

To understand more about this study, looking to the descriptive Table 3, will confer a deep understanding about the behavior of the respondents. Taking into consideration the means, the participants reacted negatively to being presented to Control ($M_{Control}$=4.05; SD=1.85) comparing to not being presented to information regarding the collection of data ($M_{Baseline\ Control\ Group}$=4.48 ; SD=1.40), which can indicate that the feeling of vulnerability was bigger because the means to control information were disclosed to the consumers, focusing on the danger that could occur but not giving all the means to perform a rational decision. Leading to the customer to perceive that while disclosing this options, consumers might need to use them someday. Focusing on the other groups, we can see positive effects with the presence of Transparency, both on the Transparency and the Control x Transparency Groups we can see an increase of Trust comparing to the Baseline Control Group. ($M_{Transparency}$=4.6; SD=1.22) and $M_{Control\ x\ Transparency}$=4.54; SD=1.38)

		N	Média	Estatística do teste Desvio	Estatística do teste Padrão	Limite inferior	Limite superior	Mínimo	Máximo
Trust	0	40	4,4875	1,40278	0,22180	4,0389	4,9361	1,50	7,25
	1	40	4,0500	1,85120	0,29270	3,4580	4,6420	1,00	7,00
	2	40	4,6000	1,21792	0,19257	4,2105	4,9895	1,50	6,25
	3	40	4,5375	1,38044	0,21827	4,0960	4,9790	1,00	6,75
	Total	160	4,4188	1,48381	0,11731	4,1871	4,6504	1,00	7,25

Table 3 - Descriptive table of Trust

Participants were also asked to measure the level of transparency and control that they've felt that their scenario had, to better understand their perceptions to each case, and analyze if the consumers perceived correctly Transparency and Control that was transmitted.

Testing ANOVA in Table 4, we can conclude that for recognizing Transparency $F_{(3,156)}$=0.112; p=0.953; η^2=0.223 we can verify that participants didn't recognize Transparency in the cases where sentences referring to Transparency were present. For Control the case is similar, with $F_{(3,156)}$=0.152; p=0.928; η^2=0.347. Meaning that we can affirm that statistically the presence of Transparency or Control didn't had a significant impact on Trust.

		Estatística de Levene	df1	df2	Sig.
Transparency	Com base em média	0,778	3	156	0,508
	Com base em mediana	0,860	3	156	0,463
	Com base em mediana e com gl ajustado	0,860	3	155,921	0,463
	Com base em média aparada	0,832	3	156	0,478
Control	Com base em média	1,617	3	155	0,188
	Com base em mediana	1,518	3	155	0,212
	Com base em mediana e com gl ajustado	1,518	3	147,662	0,212
	Com base em média aparada	1,664	3	155	0,177

Table 4 - ANOVA test description of Transparency and Control

To analyze the effect of Trust in Gender, a 2-way ANOVA was conducted, that verifies the previous test, and implies that Gender didn't had an influence in the results, as exhibited in the previous one-ANOVA test, on any case, p=0.4 > 0.05. Illustrated by Table 5, p= 0.586 > 0.05 for Gender and in case there was doubts, the different cases did not have significant differences as well p=0.349 > 0.05.

Tests of Between-Subjects Effects

Dependent Variable: Trust

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	14.557a	7	2,080	0,942	0,476
Intercept	2746,822	1	2746,822	1244,418	0,000
Gender	0,658	1	0,658	0,298	0,586
Case	7,311	3	2,437	1,104	0,349
Gender * Case	6,546	3	2,182	0,989	0,400
Error	335,512	152	2,207		
Total	3474,125	160			
Corrected Total	350,069	159			

a. R Squared = .042 (Adjusted R Squared = -.003)

Table 5 - Tests of Between-Subjects Effects two-way ANOVA

Focusing on the average scores that respondents gave on Transparency and Control, illustrated in Table 6, can conclude that when asked about Transparency, the presence of suppressors did increase their perception of Transparency, although when facing only Control, this effect still happens which leads to recognize that by approaching the consumer with information, even if it is just to explain that consumers having opt-out options, helps the perception of the consumer on the transparency of the company. Both Transparency and Control statement although has a positive Transparency recognition isn't affected as the same way as the Transparency and Control statements.

In the case of Control, the effect was completely different. Respondents felt more Control when a statement regarding their privacy wasn't shown, even more than when Control only was or when both suppressors where present in the message. From the three scenarios with suppressors, the one that lead to higher respondents' perceptions regarding Control was the Transparency statement.

		N	Média	Estatística do teste Desvio	Estatística do teste Padrão	Limite inferior	Limite superior	Mínimo	Máximo
Transparency	0	40	4,68	1,289	0,204	4,26	5,09	1	7
	1	40	4,80	1,572	0,249	4,30	5,30	1	7
	2	40	4,85	1,388	0,219	4,41	5,29	1	7
	3	40	4,75	1,391	0,220	4,31	5,19	1	7
	Total	160	4,77	1,402	0,111	4,55	4,99	1	7
Control	0	40	4,55	1,358	0,215	4,12	4,98	1	7
	1	40	4,43	1,708	0,270	3,88	4,97	1	7
	2	39	4,46	1,448	0,232	3,99	4,93	1	7
	3	40	4,33	1,509	0,239	3,84	4,81	1	7
	Total	159	4,44	1,499	0,119	4,21	4,68	1	7

Table 6 - Descriptive table of Transparency and Control

4.2.5. Discussion

Study 1 provides evidence that doesn't support our proposed model, on the contrary, it implies that while being exposed to privacy statements regarding any nature the effects are not significant to change or mitigate the effects of Data Access Vulnerability on Trust. It proves as well, that the participants didn't acknowledge the difference between having transparency or control in their booking process, invalidating the hypothesis 1,2 and 3. Although the test doesn't verify a statistically significant effect, it could verify some kind of negative effect on Trust when in the presence of Control only.

This study 1 also indicates that besides not understanding the presence of Transparency and Control on the statements, the feeling of vulnerability isn't also mitigated by these suppressors, guiding to conclusions that it is important to understand if the Data Access Vulnerability has any impact on Trust on the Hotel Industry, more specific on a moderate level of trust hotel such as Accor. Which leads to Study 2.

4.3. STUDY 2

4.3.1. Participants and Design

Sixty nine respondents voluntarily participated in a scenario-based experiment (71,7% percent women), with a single factorial design, where the participants were asked to evaluate the level of Trust on Accor Hotels, before and after the request for their data while being in the context of booking a room on their official website.

4.3.2. Procedure

Participants were firstly asked to refer if they knew the brand and to evaluate the Trust that they have in Accor Hotels, using the same scale for Trust that it was used in Study 1, afterwards they are asked to imagine a scenario where they were booking a room in Accor Hotels' Official Website and were asked to release information, such as Name, Country, Phone Number, Email and Credit Card Number as part of the reservation process adapted from other researches (Martin, Borah & Palmatier, 2017; Lee, Au & Law, 2012). This request on the contrary of Study 1 wasn't followed by any privacy statements. After being presented the scenario were asked to rank their levels of Trust after this request.

Demographic information which included age, gender and level of education was requested and before completing the survey, participants were asked to rate the level of Transparency and Control that they have perceived in the scenario experienced.

4.3.3. Measures

The Measures applied were the same of the Study 1 to guarantee the accordance between studies, by having Trust as the main dependent variable in Study 2 as well. Participants indicated their level of

Cognitive Trust by answering to 4 questions: “I trust Accor Group”, “Accor Group is very trustworthy”, “I have confidence in the Accor Group’s behaviours”, “Accor Group is reliable” Answers were coded from 1 (strongly disagree) to 7 (strongly agree) scale, adapted from Martin, Borah & Palmatier, 2017.

4.3.4. Findings

After Study 1 proved that the suppressors didn’t had any impact mitigating the Data Access Vulnerability negative impacts on Trust, it is important to understand if there is any Data Access Vulnerability feeling in a brand with middle level of trust such as Accor. To do it respondents were asked to classify the level of Trust before and after experiencing booking a room at Accor Hotels’ Website. To be able to test the scenarios and see if there is any significant difference between samples, we have to use the T-student’s test with dependent variables.

To be able to proceed with this test, there are some assumptions that need to be complied with, the first assumption is that the sample must follow the Normal Distribution, which is compiled since it has a sample bigger than 25, the dependent variable should be continuous and the independent variable can be 2 different time periods, in this case it is previous to the request of data and after, to cease there shouldn’t be any outliers.

Scrutinizing the T-student’s test, taking into consideration Table 7, the test shows that $T_{(68)}= 0.230$, $p=0.819$; $p>0.05$, meaning that with statistically significance we can affirm that there isn’t a significant difference between the Trust in brand before and after the request of data, leading to conclusions that the Data Access Vulnerability in the Hotel Industry, more specifically a middle level Trust brand such as Accor Hotels, doesn’t have an impact on Trust.

Paired Samples Test

		Paired Differences							
					95% Confidence Interval of the Difference				
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper	t	df	Sig. (2-tailed)
Pair 1	Trust Before-Trust After	0,02174	0,78560	0,09458	-0,16698	0,21046	0,230	68	0,819

Table 7 - Paired Samples Test for Trust Before and After Data Request

Taking a look into the descriptive of both Trust before and after Data Access Vulnerability, through Table 8 it is identified that Trust is affected by Data Access Vulnerability using the Accor Hotels Brand. As described below, the Trust before suffers a minor impact after the request for information, ($M_{\text{Trust Before}}=4.75$; $SD= 0.96$; $M_{\text{Trust After}}=4.73$; $SD=1.14$) but as mentioned through the T-Student’s test this impact doesn’t offer Statistically Significance.

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Trust Before	4,7536	69	0,96109	0,11570
	Trust After	4,7319	69	1,14750	0,13814

Paired Samples Statistics

Table 8 - Descriptive Statistics of Trust Before and After Request

An important learning from this study is that Accor Hotels Brand, being a middle average trusted brand has a similar percentage of identification in the mind of the consumer, meaning that only 53,6% of the respondents knew the brand.

4.3.5. Discussion

Study 2 provided evidence that supports the results on Study 1, showing that on the contrary of the proposed model, the effects of Data Access Vulnerability on Trust are so low or non-existent that the inclusion of suppressors won't affect this relationship (Martin, Borah & Palmatier, 2017).

Adding the confirmation that in the Hotel Industry, when dealing with an average trusted brand, the practice of disclosing personal information is seen as needed and relevant which doesn't raise any feeling of vulnerability on the consumer, but also reinforcing the state of privacy paradox.

5. GENERAL DISCUSSION

The present research clarifies that while analyzing the negative effects of Data Access Vulnerability on Trust, the suppressors didn't had the expected impact on mitigating them.

Although it has been proved that the suppressors have positive effects on mitigating the negative effects of Data Access Vulnerability, the prior studies, didn't focused on the Hotel Industry.

Being subject of tests, the results showed that our previous stated hypotheses should be rejected, indicating that in a middle trusted brand such as Accor, neither Transparency, Control or both of them would change the negative impacts on Trust, which could happen because of the consumers' lack of perception on understanding privacy statements, meaning that although the research followed other researches to maintain a clear and simple language, the consumers still had a certain difficulty to understand it. Other variable that could influence the lack of the suppressor's effect is that there isn't a way to guarantee that the consumers are reading them, as shown in prior researches (Lee, Au & Law, 2012), but also it could mean that only Transparency and Control wouldn't be enough to mitigate the effect of Data Access Vulnerability and other variables should also be taken into consideration to make sure that the consumer is fully empowered.

With so many questions unanswered, the need to understand if the Hotel Industry suffered from any level of Data Access Vulnerability, as stated in previous researches, more specifically an middle average trusted brand such as the Accor Hotels Brand was imperative, which lead to Study 2.

Study 2 explained one of the reasons that support the non-significant impact of the suppressors which is possibly also the most relevant one for these hypotheses' rejection. Within the context that in the presence of brands such as Accor Hotels, the request for information had no significant impact on the consumers' trust, justifying partially the null impact of suppressors.

Also both studies brought to light the need to comprehend more about what consumers feel that concepts such as Transparency and Control are, implicating that by clarifying the users ability to change privacy settings, could be comprehended as an action of Transparency by the company, because while explaining it consumers perceived it as an explanation regarding the procedures of data collection and communication. Meanwhile both studies helped clarifying this relationship between consumer and data access vulnerability, also leading to the confirmation of the privacy paradox, in this case with real cases the respondents didn't had any trouble disclosing and their trust levels weren't impacted.

6. THEORETICAL CONTRIBUTIONS

This work deepens our understanding of Data Vulnerabilities in the Hotel setting, focusing on Data Access Vulnerabilities. The gossip theory suggests that transparency and control can suppress the negative effects of the vulnerability (Martin, Borah & Palmatier, 2017; Baker, Gentry & Rittenburg, 2005). Contrary to the proposed hypothesis, the Study 1 shows that customers don't seem to react differently to the request of their personal information while being exposed to the suppressors of Transparency and Control in a booking process. A possible explanation for such finding is that, when data access vulnerability is already low, these perceptions are likely weak anyway, having a low effect on trust (Martin, Borah & Palmatier, 2017). To test this effect, Study 2 lead us on a confirmation that while being standard to self-disclosure on booking a hotel this might lead to that after choosing the hotel brand and the location, the vulnerability won't affect the decision to complete the booking or in any case the level of vulnerability is so low that it won't impact levels of Trust. Although data vulnerabilities have been studied, most previous studies are limited by general studies, without a clear distinction of industry and without focusing on tourism (Martin, Borah & Palmatier, 2017). A prior study was done regarding trust, but was referring to the privacy policies and it's formats, only implying that the mere presence of privacy policies does not guarantee that customers will read them (Lee, Au & Law, 2012). Those studies didn't include the clear communication of data procedures before the process of booking. in Study 1, we acknowledged that in all scenarios, the participants didn't notice the presence of either Transparency or Control which can lead to conclusions regarding understanding and acknowledge what privacy statements contain. Besides extending Gossip Theory this study included two other theories, the CPM theory and the T's-form theory, which helped on creating a bigger understanding regarding the creation of a positive and free of vulnerabilities communication flow between company and consumer. Although it evaluates some of the same variables that Gossip Theory does, it allows a more comprehensive description of them, and adds the perspectives of relevance that can be perceived on the request of such sensitive data as it is in a booking process (Mazurek & Malagocka, 2019).

The research can imply as well, that although on surveys individuals express privacy concerns regarding their data, when confront to a real case scenario they trust isn't impacted by vulnerability and they proceed without any changes, confirming that the privacy paradox is indeed an element to take into consideration and that the reciprocity theory is an important variable to take into consideration, because while booking an hotel the need to provide information can be seen as a step to have access to enjoy the service (Mazurek, G., Malagocka, K.,2019; Schumann, Wangenheim & Groene, 2014; Alpizar, Carlson & Johansson-Stenman, 2008).

7. MANAGERIAL IMPLICATIONS

Our findings provide evidence which denies that Data Access Vulnerability effect on Trust is mitigated by the suppressors on the Hotel industry, even with the increase of privacy concerns. Comparing the scenarios with and without the suppressors, the study's findings suggest that the significance in the impact from Data Access Vulnerability on Trust is non-existent.

Based on the study, we can suggest that managers from Brands where trust is already perceived, such Accor Hotels, do not need to prioritize the privacy policies to highlight suppressors such Transparency and Control at a booking phase, since there are not any guarantees that the statements are read and clearly understood (Lee, Au & Law, 2012).

Although proving that the data access vulnerability does not have an high impact on Trust, even without the Suppressors, we suggest that companies do not forget their responsibilities towards the consumers.

We also suggest that they should follow the procedures of GDPR for legal purposes, which involves giving transparency and some means of control to the consumers, such as opt-out options, by doing this they will also protect themselves from possible fines (Schweigert & Geyer-Schulz, 2019).

If companies do not do it for privacy concerns or because of the impact that the suppressors can mitigate in the vulnerability feeling, companies should do it as a strategy to strengthen the perception of privacy. By using it as a strategy, hotel brands are reinforcing privacy practices that will most likely benefit their overall brand perception. This strategy even in an industry that the request for information is mandatory to proceed and to take advantage of a service, can be seen as a competitive advantage (Redman & Waitman, 2020; Martin & Murphy, 2017).

To conclude it is important that companies keep finding new ways to mitigate any kind of privacy related concern, even with finding different variables besides Transparency and Control, or finding different formats to the statements, such as videos in order to prevent consumers' concerns to be an issue during bookings.

8. LIMITATIONS AND FUTURE RESEARCH

Considering the lack of research on Data Vulnerabilities, this study provides a path for future research. In our Study, we chose to focus on Data Access Vulnerability on hotel industry. Future research should extend this line of inquiry to other types of Data Vulnerabilities, such as Data Manifest Vulnerability and Data Breach Vulnerability.

Further, future research should measure this impacts for other hotel brands, since Accor Group is an established brand with an average Trust among consumers and for how the GDPR laws manage to soften the perception of vulnerability effect on Trust, allowing a precondition of safety for any hotel brand.

This research focuses on two suppressors - transparency and control that is based on the conceptual framework of Gossip Theory, which refers to how people respond to the unsanctioned collection (Martin, Borah & Palmatier, 2017), other frameworks should be tested, in this case CPM and T-form's theory has other variables such as Pre-notion of Trust and relevance of the information requested.

Future researches should focus also on how different people react differently to Data Access Vulnerability, based on consumers' characteristics, knowing that more experienced people on making online hotel bookings, tend to be less concerned about online privacy (Lee, Au & Law, 2012).

At last, other variable that could be analyzed is the presence of online reviews and how it could impact and mitigate the vulnerability feeling on the consumers, since that part of the trust that consumers have on a brand is now from the research of online reviews.

9. BIBLIOGRAPHY

Acquisti, A., & Varian, H. (2005). Conditioning prices on purchase history. Marketing Science, 24, 367–381.

Aguirre, E., Mahr, D., Grewel, D., Ruyter, K. D., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. Journal of Retailing, 91, 34–59.

Alpizar, Francisco, Fredrik Carlsson, and Olof Johansson-Stenman (2008), "Anonymity, Reciprocity, and Conformity: Evidence from Voluntary Contributions to a National Park in Costa Rica," Journal of Public Economics, 92 (5/6), 1047–60.

Anderson, C. (2013), "Identity Theft Growing, Costly to Victims," USA Today (April 14), http://www.usatoday.com/story/ money/personalfinance/

Anderson, L. & Ostrom, A.L. (2015). Transformative service research: Advancing our knowledge about service and well-being. Journal of Service Research, 18(3), 243--249.

Anderson, L., Ostrom, A. L., & Bitner, M. J. (2011). Surrounded by services: A new lens for examining the influence of services as social structures on well-being (Working paper). W. P. Carey School of Business, Arizona State University.

Baker, S., Gentry, J., Rittenburg, G. (2005). Building Understanding of the Domain of Consumer Vulnerability. Journal of Macromarketing, 25, 128-139.

Bart, Y., Shankar, V., Sultan, F., Urban, G. (2005) Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. Journal of Marketing, 69, 133-152.

Barth, S., & Jong, M.D. 2017. "The Privacy Paradox—Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review." Telematics and Informatics 34 (7): 1038–1058

Bauman, A., & Bachmann, R. (2017). Online Consumer Trust: Trends in Research. Journal of Technology Management & Innovation, 12(2), 68-79. doi:10.4067/s0718-27242017000200008

Beersma, B., & Kleef, G. A. (2012). Why People Gossip: An Empirical Analysis of Social Motives, Antecedents, and Consequences. Journal of Applied Social Psychology, 42(11), 2640-2670. doi:10.1111/j.1559-1816.2012.00956.x

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced Confidences. Social Psychological and Personality Science, 4(3), 340-347. doi:10.1177/1948550612455931

Brehm, Jack W. (1989), "Psychological Reactance: Theory and Applications," in Advances in Consumer Research, Vol. 16, Thomas K.Srull, ed. Provo, UT: Association for Consumer Research, 72–75.

Browne, R. (2020, January 20). Europe's privacy overhaul has led to $126 million in fines - but regulators are just getting started. Retrieved May 24, 2020, from https://www.cnbc.com/2020/01/19/eu-gdpr-privacy-law-led-to-over-100-million-in-fines.html

Cheng, X. & Walton, S. (2019). Do Nonprofessional Investors Care About How and When Data Breaches are Disclosed? Journal of Information Systems, 33(3), 163-182

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. Health Services Research, 54(5), 971-980. doi:10.1111/1475-6773.13203

Clee, Mona A. and Robert A. Wicklund (1980), "Consumer Behavior and Psychological Reactance," Journal of Consumer Research, 6 (4), 389–405.

Cohen, Julie E. (2012). "What Privacy Is For." Harvard Law Review no. 126: 1904–1933.

Columbus, L. (2017), " 53% Of Companies are adopting big data analytics", Forbes, (December, 24), https://www.forbes.com/sites/louiscolumbus/2017/12/24/53-of-companies-are-adopting-big-data-analytics/#79c7cc8c39a1

Conti, G., & Sobiesk, E. (2010). Malicious interface design: Exploiting the user. In Proceedings of the 19th International Conference on World Wide Web (pp. 271e280). New York, NY: Association for Computing Machinery.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. Information Systems Research, 17(1), 61–80.

Echeverri, P. & Salomonson, N. (2019). Consumer vulnerability during mobility service interactions: causes, forms and coping. Journal of Marketing Management, 35, 364-389.

Emler, Nicholas (1994), "Gossip, Reputation and Social Adaption,"in Good Gossip, R.F. Goodman and A. Ben-Ze'ev, eds. Lawrence: University of Kansas Press, 119–40.

Etzioni, A. (2017). Cyber Trust. Journal of Business Ethics, 156(1), 1-13

Fox, C. (2019, January 21). Google hit with £44m GDPR fine over ads. Retrieved May 24, 2020, from https://www.bbc.com/news/technology-46944696

Foxman, E. R., & Kilcoyne, P. (1993). Marketing practice, and consumer privacy: Ethical issues. Journal of Public Policy & Marketing, 12, 106–119.

Godin, S. (2007). Permission marketing: turning strangers into friends, and friends into customers. London: Pocket.

Goldfarb, A., & Tucker, C. (2011). Online display advertising: targeting and obtrusiveness. Marketing Science, 30, 389–404.

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. Management Science, 57, 57–71.

Gwebu, K. L., J. Wang, and W. Xie. (2014). Understanding the Cost Associated with Data Breaches. Proceedings of the Pacific Asia Conference on Information Systems.

Hsieh, J., & Li, Y. (2020). Will You Ever Trust the Review Website Again? The Importance of Source Credibility. International Journal of Electronic Commerce, 24(2), 255-275. doi:10.1080/10864415.2020.1715528

Izogo, E. E., Jayawardhena, C., & Adegbola, E. A. (2018). Creating particularized trust in e-retailers through experiential value and generalized trust. Journal of Strategic Marketing, 28(1), 16-38.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. Journal of Marketing, 82(2), 85-105. doi:10.1509/jm.16.0124

Jiang, Z. J., Heng, C. S., & Choi, B. C. F. (2013). Research note —privacy concerns and privacyprotectivebehaviorinsynchronousonlinesocialinteractions.InformationSystemsResearch,24(3), 579–595.

John, L., Acquisiti, A., Loewenstein, G. (2011). Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information.Journal of Consumer Research, 37, 858-873.

Johnson, D., and K. Grayson. (2005). “Cognitive and Affective Trust in Service Relationships.” Journal of Business Research 58:500–7.

Kang, J. (1998). Information privacy in cyberspace transactions. Stanford Law Review, 50, 1193–1294.

Kim, D.J., Ferrin, D. L., & Rao, H.R.(2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. Information Systems Research, 20(2), 237-257.

Kim, M., & Kim, J. (2019). The Influence of Authenticity of Online Reviews on Trust Formation among Travelers. Journal of Travel Research, 59(5), 763-776. doi:10.1177/0047287519868307

Krafft, M., Arden, C., & Verhoef, P. (2017). Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions?. Journal Of Interactive Marketing, 39, 39-54.

Kumar, V., Zhang, X., Luo, A. (2014). Modeling Customer Opt-In and Opt-Out in a Permission-Based Marketing Context. Journal of Marketing Research, 51, 403-419.

Lawrence, A., M. Minutti-Meza, and D. Vyas. 2018. Is operational control risk informative of undetected financial reporting deficiencies? Auditing: A Journal of Practice & Theory 37 (1): 139–165. https://doi.org/10.2308/ajpt-51784

Layton, R., and P. A. Watters. 2014. A methodology for estimating the tangible cost of data breaches. Journal of Information Security and Applications 19 (6): 321–330. https://doi.org/10.1016/j.jisa.2014.10.012

Lee, H.,A, Au, N., Law, R.(2012).Presentation Formats of Policy Statements on Hotel Websites and Privacy Concerns: A multimedia learning Theory Perspective.Journal of Hospitality & Tourism Research, 37, 470-489.

Lehto, X. Y., Kim, D. Y., & Morrison, A. M. (2006). The effect of prior destination experience on online information search behavior. Tourism and Hospitality Research, 6(2), 160-178.

Lehto, X. Y., Kim, D.-Y., & Morrison, A. M. (2006). The Effect of Prior Destination Experience on Online Information Search Behaviour. Tourism and Hospitality Research, 6(2), 160–178.

Lewis, J.D., Weigert, A., 1985. Trust as a social reality. Soc. Forces 63 (4), 967–985.

Lien,C., Wen, M., Huang,L., Wu, K. (2015). Online hotel booking:The effects of brand image, price, trust and value on purchase intentions. Asia Pacific Management Review, 20, 210-218.

Lock, D. (1997). The Gower handbook of management. Aldershot: Gower.

Lwin, May, Jochen Wirtz, and Jerome D. Williams (2007), "Consumer Online Privacy Concerns and Responses: A Power–Responsibility Equilibrium Perspective," Journal of the Academy of Marketing Science, 35, 4, 572–85.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns: The construct, the scale, and a causal model. Information Systems Research, 15, 336–355.

Martin, K. (2019). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. Business Ethics Quarterly, 30(1), 65-96

Martin, K., Borah, A., Palmatier, R. (2017). "Data Privacy : Effects on Customer and Firm Performance", Journal of Marketing, 81 (January), 36-58

Martin, K., Murphy, P. (2017). "The role of Privacy in Marketing". Journal of the Academy Marketing Science, 45, 135-155.

Mayer, R. C., Davis, J. H., Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), 709. doi:10.2307/258792

Mazurek, G.,Malagocka, K. (2019). What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think. Business Horizons, 62, 751-759.

Michael, S. (2019). Marriott Starwood hotel data breach FAQ: What 500 million ... Retrieved May 21, 2020, from https://www.pcworld.com/article/3324609/marriott-starwood-hotel-data-breach-faq.html

Milne, G., Boza, M. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. Journal of Interactive Marketing, 13, 5-24.

Mishra, S., Wiley, J., Gardner, M., Coughlan, A., Howell, R. (2000). "....New Books In Review". Journal Of Marketing Research, 37, 525-526.

Moon, Y. (2000), "Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers",Journal Of Consumer Research, 26 (March), 323 - 334.

Moorman, C., Deshpandé, R. & Zaltman,G. (1993), "Factors Affecting Trust in Market Research Relationships," Journal of Marketing, 57 (January), 81–101.

Morgan, R. Hunt, S. (1994) The Commitment-Trust Theory of Relationship Marketing. Journal of Marketing, 58(3), 20-38.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. Journal of Marketing, 58(3), 20–38. doi:10.2307/1252308

Morgan, S. (2017). Cybercrime to $6 trillion by 2021. Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report2016/

Moschis, G. P. (1992). Marketing to older consumers: A handbook of information for strategy development. Westport, CT: Quorum Books.

Nill, A., & Aalberts, R. J. (2014). Legal and ethical challenges of online behavioral targeting in advertising. Journal of Current Issues and Research in Advertising, 35, 126–146.

Nissenbaum, Helen. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.

O'Connor, P., & Frew, A. J. (2004). An evaluation methodology for hotel electronic channels of distribution. International Journal of Hospitality Management, 23(2), 179–199.

O'Connor, P., & Frew, A. J. (2004). An evaluation methodology for hotel electronic channels of distribution. International Journal of Hospitality Management, 23(2), 179-199. doi:10.1016/j.ijhm.2003.10.002

Palmatier, R. W., & Martin, K. D. (2019). The intelligent marketers guide to data privacy: the impact of big data on customer trust. Cham, Switzerland: Palgrave Macmillan.

Perrin, A. (2020, April 14). Half of Americans have decided not to use a product or service because of privacy concerns. Retrieved May 20, 2020, from https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/

Petronio, S. & Gaff C. (2010). Managing privacy ownership and disclosure. Family Communication About Genetics: Theory and Practices. Oxford University Press, 120-135.

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. New York, USA: State University of New York Press.

Petronio,S. & Child, J. (2020). Conceptualization and operationalization: utility of communication privacy management theory. Current Opinion in Psychology, 31, 76-82.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing, 19(1), 27-41. doi:10.1509/jppm.19.1.27.16941

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. Journal of Business Ethics, 62(3), 221–235.

Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: Socio-demographic and attitudinal influences on privacy and disclosure choices. Journal of Marketing Management, 36(5-6), 519-549. doi:10.1080/0267257x.2020.1715465

Privacy Rights Clearinghouse. (2006). What to do when you receive a data breach notice. Retrieved May 24, 2020, from https://privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice

Redman, T., Waitman, R. (2020, January 28). Do You Care About Privacy as Much as Your Customers Do? Hardvard Business Review.

Regan, Priscilla M. (1995). Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill, NC: University of North Carolina Press.

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. Journal of Information Systems, 33(3), 227-265. doi:10.2308/isys-52379

Scharf, S. (2007), “Report Casts Doubt on the Impact of Data Breaches on Identity Theft,” Internal Auditor, 64 (4), 23.

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting Web Site Visitors into Buyers: How Web Site Investment Increases Consumer Trusting Beliefs and Online Purchase Intentions. Journal of Marketing, 70(2), 133-148. doi:10.1509/jmkg.70.2.133

Schumann, J., Wangenheim, F., Groene, N. (2014).Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance Among Users of Free Web Services. Journal of Marketing, 78, 59-75.

Schweigert, V., & Geyer-Schulz, A. (2019). The Impact of the General Data Protection Regulation on the Design and Measurement of Marketing Activities: Introducing Permission Marketing and Tracking for Improved Marketing & CRM Compliance with Legal Requirements. Journal of Marketing Development and Competitiveness, 13(4).

Sheehan, Kim B. and Mariea G. Hoy (1999), “Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns,” Journal of Advertising, 28, 3, 37–51.

Simpson, J. A. (2007). Psychological foundations of trust. Current Directions in Psychological Science, 16(5), 264–268. doi:10.1111/j.1467-8721.2007.00517.x

Smith, C., and Cooper-Martin, E. (1997), “Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability,” Journal of Marketing, 61 (July), 1–20.

Smith, H. J., S. Milberg, S. Burke. 1996. Information privacy: Measuring individuals’ concerns about organizational practices. MIS Quart. 20(2) 167–196.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154, 477–560.

Son, Jai-Y and Sung S. Kim (2008), “Internet Users' Information Privacy-protective Responses: A Taxonomy and a Nomological Model,” MIS Quarterly, 32, 3, 503–29.

Sparks, B. A., & Browning, V. (2011). The impact of online reviews on hotel booking intentions and perception of trust. Tourism Management, 32(6), 1310-1323. doi:10.1016/j.tourman.2010.12.011

Sparks, B. A., & Browning, V. (2011). The impact of online reviews on hotel booking intentions and perception of trust. Tourism Management, 32(6), 1310–1323.

Sterling, G. (2017), “ Millions of dollars at risk if companies don’t take consumer data protection seriously”, MarTech Today, (August, 17), https://martechtoday.com/millions-dollars-risk-companies-dont-take-consumer-data-protection-seriously-202643

Stewart, K. A., A. H. Segars. 2002. An empirical examination of the concern for information privacy instrument. Inform. Systems Res. 13(1) 36–49.

Suthaharan, S. (2018). Big data analytics: Machine learning and Bayesian learning perspectives—What is done? What is not? WIREs Data Mining and Knowledge Discovery, 9(1). doi:10.1002/widm.1283

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. Computers and Society, 31(1), 6–11.

Tezinde, T., Smith, B., & Murphy, J. (2002). Getting permission: Exploring factors affecting permission marketing. Journal of Interactive Marketing, 16(4), 28-36.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research, 22(2), 254-268. doi:10.1287/isre.1090.0260

Tsukayama, H. 2017. Why it can take so long for companies to reveal their data breaches. The Washington Post (September 8)

Tucker, Catherine (2014), “Social Networks,Personalized Advertising and Privacy Controls”, Journal of Marketing Research, 51 (October), 546-62

Westin, A. (1967). Privacy and freedom. New York: Antheneum. White, T. B. (2004). Consumer disclosure and disclosure avoidance: a motivational framework. Journal of Consumer Psychology, 14, 41–51.

Winer, R. (2009). New Communications Approaches in Marketing: Issues and Research Directions. Journal of Interactive Marketing, 23, 108-117

Wright, S. A., & Xie, G. (2017). Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations. Journal of Business Ethics, 156(1), 123-140.

Xu, H., Luo, X. (Robert), Carroll, J. M., & Rosson, M. B. (2011).The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42–52.

Yeon, J.,Parka, I.,Lee, D. (2019) What creates trust and who gets loyalty in social commerce?.Journal of Retailing and Consumer Services, 50,138-144.

10.APPENDIX

Pre-test

Thank you for agreeing to take part in this important academic survey.
Today we will be gathering some data, in order to take better conclusions regarding Trust in Brands.
This survey should only take 2-3 minutes to complete.
Please, be assured that all answers you provide will be kept in the strictest confidentiality.

Please Classify this Brands below, in terms of level of trust that you have on them:

	Much weaker									Much Stronger
	0	1	2	3	4	5	6	7	8	9	10
Pestana Hotel Group											
Vila Galé											
Tivoli Hotels											
Booking.com											
Momondo											
AirBnb											
Expedia											
HomeToGo											
Accor Hotels											
Hoti Hotéis / Meliá Hotels & Resorts											
Mariott Hotels & Resorts											
Minor Hotels											
Sana Hotels											

Which are the reasons that lead you to trust a brand?

Imagine now, that while you're booking a hotel in their website, they ask you for your data, without any more information.
The information that they ask you for is:
NAME
E-MAIL
ADDRESS
CREDIT CARD NUMBER
MOBILE NUMBER
DATE OF BIRTH
ID NUMBER

How do you measure the level of trust, after this request?

	Much Weaker									Much stronger
	0	1	2	3	4	5	6	7	8	9	10
Trust											

Gender

- ○ Male
- ○ Female

Age

- ○ Under 18
- ○ 18 - 24
- ○ 25 - 34
- ○ 35 - 44
- ○ 45 - 54
- ○ 55 - 64
- ○ 65 - 74
- ○ 75 - 84
- ○ 85 or older

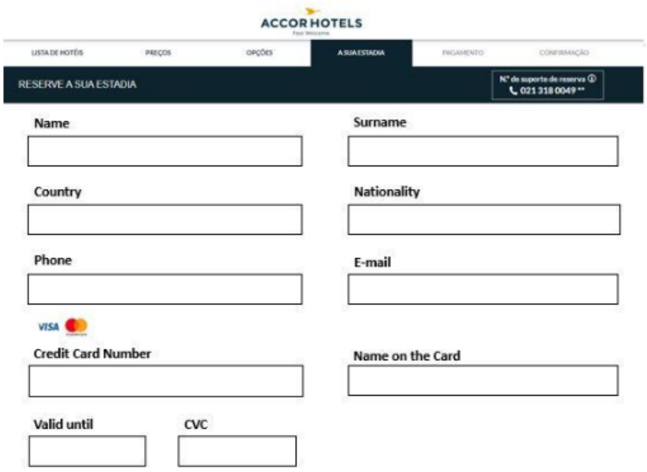
Education

- ○ Less than high school
- ○ High school graduate
- ○ Bachelor
- ○ Masters
- ○ Doctorate
- ○ Other

Study 1

Thank you for taking part in this survey.
By participating in this study with the purpose of understanding how people perceive Data Collection and how they evaluate the impact on Brand Trust, you are agreeing to let us use the answer to the following questions exclusively for academic research.
You have to be 18 years old or older to be able to participate.

Imagine that you're going on vacations with your family and you're the one in charge of making the Group's Reservation.
After deciding the destination you chose to try and book with the Hotel Chain Accor Hotels.
While trying to make a reservation, the following Information was requested:


ACCOR HOTELS

LISTA DE HOTÉIS | PREÇOS | OPÇÕES | A SUA ESTADIA | PAGAMENTO | CONFIRMAÇÃO

RESERVE A SUA ESTADIA

Nº de suporte de reserva
021 318 0049 **

Name

Surname

Country

Nationality

Phone

E-mail

VISA

Credit Card Number

Name on the Card

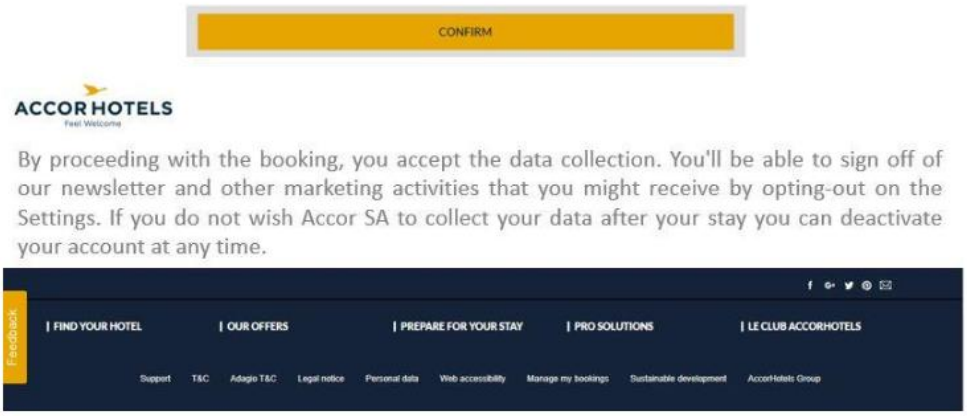
Valid until

CVC

Please select the option that best describes how you feel about the following sentences:

	Strongly Disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
I Trust Accor Group							
Accor Group is very trustworthy							
I have confidence in the Accor Group's Behaviors							
Accor Group is reliable							

At the End of the requested information you find the following:



Please select the option that best describes how you feel about the following sentences:

	Strongly Disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
I Trust Accor Group							
Accor Group is very trustworthy							
I have confidence in the Accor Group's Behaviors							
Accor Group is reliable							

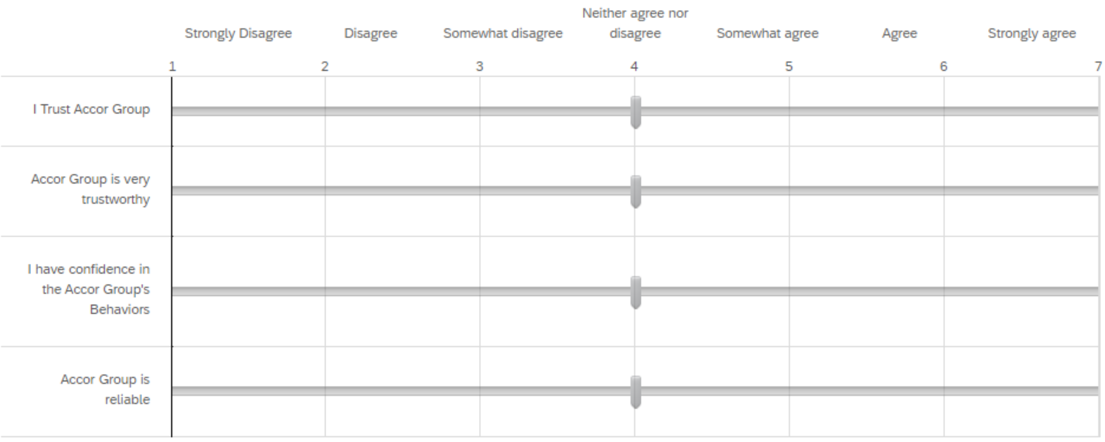
At the End of the requested information you find the following:

ACCORHOTELS

Feel Welcome

The Data collected are processed by Accor SA and are needed to be able to manage the booking request, know you better and communicate information about products and services from Accor Group. This information won't be shared with any third party that doesn't belong to Accor SA.

Please select the option that best describes how you feel about the following sentences:



At the End of the requested information you find the following:

ACCORHOTELS

Feel Welcome

The Data collected are processed by Accor SA and are needed to be able to manage the booking request, know you better and communicate information about products and services from Accor Group. This information won't be shared with any third party that doesn't belong to Accor SA.

By proceeding with the booking, you accept the data collection. You'll be able to sign off of our newsletter and other marketing activities that you might receive by opting-out on the Settings. If you do not wish Accor SA to collect your data after your stay you can deactivate your account at any time.

Please select the option that best describes how you feel about the following sentences:

	Strongly Disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
I Trust Accor Group							
Accor Group is very trustworthy							
I have confidence in the Accor Group's Behaviors							
Accor Group is reliable							

Age

- ○ 18 - 24
- ○ 25 - 34
- ○ 35 - 44
- ○ 45 - 54
- ○ 55 - 64
- ○ 65 - 74
- ○ 75 - 84
- ○ 85 or Older

Gender

- ○ Male
- ○ Female

Education

- ○ Less than High School
- ○ High School Graduate
- ○ Bachelor
- ○ Masters
- ○ Post Graduate
- ○ Doctorate

Rate the Previous Scenario Scenario in terms of:

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
Transparency							
Control							

Study 2

ACCOR HOTELS
Feel Welcome

Please select the option that best describes how you feel about the following sentence "I know the Accor Hotels Brand"

Yes	No
○	○

Please select the option that best describes how you feel about the following sentences:

	Strongly Disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
I Trust Accor Group							
Accor Group is very trustworthy							
I have confidence in the Accor Group's Behaviors							
Accor Group is reliable							

Imagine that you're going on vacations with your family and you're the one in charge of making the Group's Reservation.
After deciding the destination you chose to try and book with the Hotel Chain Accor Hotels.
While trying to make a reservation, the following Information was requested:

ACCOR HOTELS

LISTA DE HOTÉIS | PREÇOS | OPÇÕES | A SUA ESTADIA | PAGAMENTO | CONFIRMAÇÃO

RESERVE A SUA ESTADIA

Nº de suporte de reserva
021 318 0049 **

Name

Surname

Country

Nationality

Phone

E-mail

VISA

Credit Card Number

Name on the Card

Valid until

CVC

Please select the option that best describes how you feel about the following sentences:

	Strongly Disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
I Trust Accor Group							
Accor Group is very trustworthy							
I have confidence in the Accor Group's Behaviors							
Accor Group is reliable							

Age

- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65 - 74
- 75 - 84
- 85 or Older

Gender

- Male
- Female

Education

- Less than High School
- High School Graduate
- Bachelor
- Masters
- Post Graduate
- Doctorate

Rate the Previous Scenario in terms of:

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
	1	2	3	4	5	6	7
Transparency							
Control							