Does My Smart Device Provider Care About My Privacy? Investigating Trust Factors and User Attitudes in IoT Systems

OKSANA KULYK, IT University of Copenhagen
KRISTINA MILANOVIC, Imperial College London
JEREMY PITT, Imperial College London

With the wide spread of IoT devices, smart systems gain more and more control over personal data and daily lives of their users. This control, however, can easily be misused, either by system providers themselves acting in bad faith, or by external attackers. Implementing proper measures towards security and privacy protection of smart systems, therefore, becomes of critical importance. In this paper we present a study to investigate beliefs among end users, whether the smart system providers are both capable and motivated to implement such measures. For this purpose, we conduct an online survey of 98 participants from the UK, which we analyse using quantitative and qualitative methods. Our results show that users' trust in proper security and privacy protection in smart systems is influenced by a multitude of factors such as information about concrete technologies and privacy policies of the systems, but also information about the company such as its reputation or geographical location. We conclude that transparency by companies, regarding both the technologies behind the concrete system and the general practices of the company itself, is a crucial factor in ensuring end user confidence.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: IoT, Smart Home, Smart Health, Security, Privacy, Trust, User Study

ACM Reference Format:
Oksana Kulyk, Kristina Milanovic, and Jeremy Pitt. 2020. Does My Smart Device Provider Care About My Privacy? Investigating Trust Factors and User Attitudes in IoT Systems. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20), October 25–29, 2020, Tallinn, Estonia.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3419249.3420108

1 INTRODUCTION

Smart systems are becoming more widespread, with a variety of devices and functions that are supposed to bring many benefits, from convenience in daily tasks to more accessible medical assistance for people who need it. Recent surveys indicate that up to 40% of UK respondents own some kind of smart home devices[15]. At the same time, as these devices are becoming more integrated in the daily lives of their users, they can pose significant security and privacy risks, either due to an external attacker or due to misuse of personal data by the system providers themselves. While a variety of both technical measures and policies have been developed to minimise such risks, a lot of trust still has to be put in the service providers who are expected to properly implement these measures. This trust is most critical for the end users of the systems, who would be the ones suffering from consequences of insufficient security and privacy

Manuscript submitted to ACM

protection. Yet, while several studies looked into the perception of the security and privacy risks in smart systems, the reasons why the end users choose to trust or distrust the systems to protect them against these risks have not been thoroughly investigated yet.

This work looks into the factors that affect how trustworthy smart system providers are perceived by their users. We focus on two aspects of trustworthiness, following the framework proposed by Riegelsberger et al. [19]: the *ability* and the *motivation* of a trustee to act according to the expectations of a person who chooses to trust or distrust the trustee. For this purpose, we conducted an online study with 98 participants which we analysed using both qualitative and quantitative methods. The results of our study show that most of the participants believe that smart systems are both capable and motivated to protect the security and privacy of their users, although there was a significant difference between types of systems (that is, between smart home and smart health systems).

We furthermore identified a number of factors that influence end users' beliefs that the service providers are capable and motivated to protect the security and privacy of their users. These factors include security and privacy policies and perceptions; financial issues; governmental regulations and other kinds of oversight; reputation; ethical issues and company profile. Alongside these factors, we identified further themes that affected participants' trust and derived recommendations to improve the trustworthiness of systems.

The paper is structured as follows. Section 2 describes the related work for the paper, including studies on trust in online systems, security and privacy decision making and mental models of security and privacy risks in IoT and smart systems. Section 3 describes the conducted study, including research questions and hypotheses. The results of the study are presented in Section 4, which describes the study procedure, followed by the discussion in Section 5 which includes recommendations for researchers and practitioners. We conclude the paper in Section 6.

2 BACKGROUND

A number of studies researched the topic of trust in online services, including trust in whether these services provide sufficient security and privacy protection. As such, Nissenbaum [17] discusses a number of challenges of trust online, such as unclear identity of the service providers, as well as factors that positively or negatively influence trust, such as history of past interactions, beliefs in the presence of enforcing mechanisms (i.e. providing accountability in case trust is violated) or social pressure. Riegelsberger et al. [19] defines a framework for trust, defining the *ability* and *motivation* of the trustee to perform the expected action, furthermore distinguishing between contextual properties (e.g. reputational loss) and intrinsic properties (e.g. trustee's benevolence) that determine whether the trustee will fulfill the trust. Further research has focused on empirical studies of factors that influence the end users trust in online services, identifying such factors as belief in presence of incentives that prevent service providers from cheating, as well as the overall design of the website of the service provider (see e.g. [9]). A comprehensive instrument has furthermore been developed by Cheung et al. [4], aimed at measuring perceived privacy and security controls of online vendors, as well as other factors such as personality and cultural traits influencing end users trust.

Further research has been dedicated to understanding the general factors that influence security- and privacy-related decision making, resulting in a variety of studies [1–3, 12, 13, 22]. The studies identified a number of diverse factors, such as perceived appropriateness of data sharing (e.g. seeing the need to share data for a specific purpose), social pressure and network effects, functionality of the service, decision biases and complexity of security and privacy controls. While some of these factors related to personality traits, knowledge and social environment of the end users, some of them focused on the context of a specific decision (i.e. the perceived appropriateness of the purpose of data

sharing) or perceived trustworthiness of the service e.g. its look and feel, perceived seriousness or information about the company behind the service.

The mental models of security and privacy in smart systems have furthermore been investigated in several studies. As such, several studies investigated security and privacy concerns and risk awareness in smart systems [8, 11, 14, 20, 23], showing that while the end users can name a variety of security and privacy risks in smart systems, many of them lack awareness about such risks. The extent to which the security and privacy concerns influence the end users decisions regarding using these systems has furthermore been investigated by Emami-Naeni et al. [5], concluding that while the end users often assign critical importance to these concerns, only few make purchasing based on these concerns. A quantitative study by Guhr and Werth [10], however, does identify an effect of privacy concerns on intention to use, together with its influence on other relevant constructs such as perceived behavioural control.

3 STUDY METHODOLOGY

We conducted an online study, the main purpose of which was to investigate the factors that influence end user's trust in the security and privacy protection of smart systems, in particular, the extent to which the users perceive the ability and the motivation of system providers to ensure the necessary protection. We consider following research questions:

- Which factors influence *the end users' beliefs* that system providers are *capable* of protecting security and privacy of their users?
- Which factors influence *the end users' beliefs* that system providers are *motivated* to protect security and privacy of their users?
- Which factors, according to the end users' beliefs, *influence the ability* of system providers to protect security and privacy of their users?
- Which factors, according to the end users' beliefs, *influence the motivation* of system providers to protect security and privacy of their users?

We conducted the investigation using a mixed methods study. In a quantitative evaluation, we studied the effect of factors such as smart system type (smart home or smart health), users' previous experience with using smart systems and users' intention to continue using smart systems based on their beliefs of the ability and motivation of smart system providers to protect their security and privacy. In order to get a better understanding on what influences the participants' beliefs we conducted a qualitative analysis of their answers.

3.1 Study Validity

For recruiting participants, we decided to use a crowd-sourcing platform. As our research design did not assume special knowledge or skills of the participants, aiming to investigate the existing mental models among general population, we deemed the use of platforms as appropriate [16]. To account for possible lack of well intention among the participants (e.g. participants aiming to skim through survey as quickly as possible in order to get their payment), we planned to filter out the responses based on the answers to open questions, excluding responses with obvious nonsense answers.

Before starting the study, the questionnaire was evaluated via pretests, obtaining feedback from experts in the field of security and privacy and human-computer interaction. It was further validated in a pilot study with five participants, also recruited from the crowd-sourcing platform we planned to use. In that way we aimed to ensure that the questions are understandable to the participants, and that the responses they provided were inline with our research questions.

3.2 Recruitment and Ethics

The participants were recruited among UK residents using the Clickworker platform[1]. They were offered a reimbursement of 2.5 Euros for their participation, which roughly corresponds to the minimal wage fee for a 15 minute study. The participants were informed about the purpose of the study, told that their responses will be kept anonymous and that they could withdraw from the study at any point.

3.3 Study Procedure

After the participants were presented with the informed consent form, they were randomly assigned to one of the two groups, either the smart home or smart health group. Each group was shown some information about the corresponding smart system (see Appendix A) and asked what their experience with using the smart system is (choosing between the options "I often use smart [system] devices", "I sometimes use smart [system] devices", "I used smart [system] devices in the past, but do not do it anymore" and "I never used a smart [system] device") and if they do not currently use the smart system, whether they want to do it in the future.

The study continued with questions about the *ability* of smart system providers to ensure security and privacy. Namely, the participants were asked to indicate whether they believed that smart system providers can protect the security and privacy of their users (using a 5-point Likert type scale) and to explain their answer via an open question. They were also asked a series of open questions, namely which factors would influence their opinion, whether there is difference in service providers' ability to protect either security or privacy, what they believed the most significant challenges faced by system providers were, and what kind of system providers they believed were either most or least capable to protect security and privacy. Similar questions were then asked about the participants' belief in the *motivation* of smart system providers to protect their security and privacy[2]. The study concluded with asking for demographic information from the participants, namely, their age group and gender.

4 RESULTS

The following section describes the results that were obtained from the study. It is broken down into three subsections which cover the demographics of the participants and the analysis of numeric answers and free-text responses of the survey.

Out of 100 participants recruited for the study, two were excluded due to either providing obviously nonsensical answers (random strings) or misunderstanding the questions. Out of the remaining 98 participants, 49 participants ended up being assigned to the smart home group and 49 were assigned to the smart health group.

4.1 Demographics

A slight majority of respondents identified as female, 53 out of 98, while 45 identified as male. Tables 1 and 2 show the age distribution and the smart system usage habits of the participants respectively. The majority of the participants who reported not currently using corresponding smart systems (including those participants who used the systems in the past and those who never used it) furthermore claimed that they would like to use them in the future (32 out of 41).

[1] https://www.clickworker.com
[2] For the list of all the questions, see Appendix B

Age range	No. participants
<20	5
20-25	13
26-35	30
36-45	27
46-55	17
56-65	4
66-75	2
>75	0

Table 1. Age distribution of participants.

Response	No. participants - Smart Home	No. participants - Smart Health
I often use smart home devices.	14	14
I sometimes use smart home devices.	16	13
I used smart home devices in the past, but do not do it anymore.	6	5
I never used a smart home device.	13	17

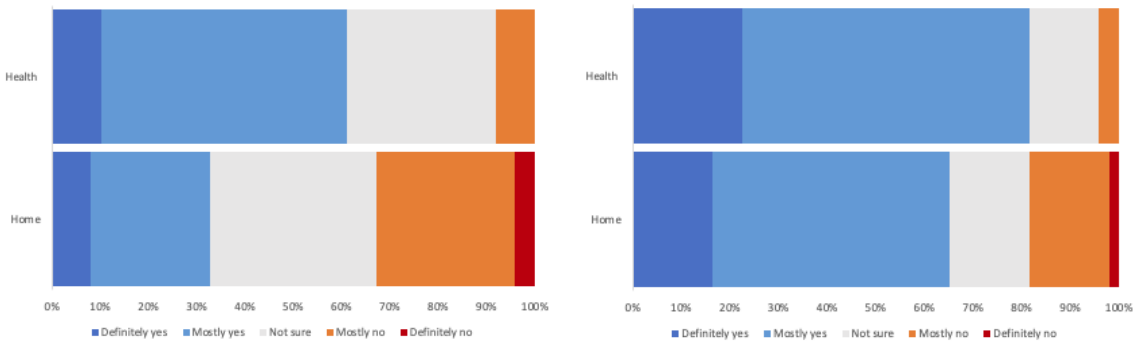
Table 2. Smart system usage habits of participants.

4.2 Analysis of Numeric Answers

The quantitative evaluation of the study considered the answers to the questions on to what extent the participants believe that the smart home and health systems protect their security and privacy. The analysis in this section concentrates on responses where participants had to supply numerical answers, for example on a Likert scale, to questions asked. The statistical analyses were done using SPSS v25 software.

4.2.1 General Ability and Motivation. Figure 1 provides the summary for ability and motivation. When it came to ability (Figure 1a), the participants in the smart health group generally felt that smart health providers were able to to protect their security and privacy, with approximately 60% of respondents believing that providers were "definitely" or "mostly" able to protect their privacy and security. By comparison, participants in the smart home group were much less confident in smart home providers ability to protect them, with only approximately 30% of participants feeling that providers were "definitely" or "mostly" able to protect their privacy and security.

The results showed that overall the majority of the participants have positive beliefs towards the motivation of smart systems in particular with more being confident in their (the smart system providers) motivation to protect users, as can be seen in Figure 1b. There are however differences between the smart home and smart health groups when it came to participants beliefs' in their ability to protect users, showing that participants in the smart health group are more confident that their data would be secure and private, as seen in Figure 1a. When asked to consider the motivation of smart health or smart home providers to protect the security or privacy of their users, the majority of participants felt that the providers were "definitiely" or "mostly"motivated to protect their users, as can be seen in Figure 1b. At the same time, the responses in our study show that there is a slightly lower level of confidence in the smart home group compared to the smart health group.



(a) Participants' attitudes towards ability.

(b) Participants attitudes towards motivation.

Fig. 1. Participants' attitudes towards ability and motivation by group (Smart Home or Smart Health).

Statistical analysis of the responses regarding ability and motivation of smart device providers to protect their users was analysed using one-way ANOVA testing[3]. When considering the *ability* of smart device providers to protect their user's security and privacy significant differences were identified between smart home and smart health groups ($F(1, 96) = 8.58$, $p = 0.002$, $\omega = 0.30$) (to 3 s.f.). This would indicate that the (random) allocation of participants to the smart health or smart home groups impacted their opinion of whether that particular smart technology was able to protect users. The effect size, $\omega = 0.030$, is approximately a medium-large effect size, $\omega^2 = 0.09$ [6].

When considering the *motivation* of smart device providers to protect their user's security and privacy significant differences were identified between smart home and smart health groups ($F(1, 96) = 3.68$, $p = 0.033$, $\omega = 0.019$) (to 3 s.f.). This would indicate that the (random) allocation of participants to the smart health or smart home groups impacted their opinion of whether that particular smart technology was able to protect users. The effect size, $\omega = 0.19$, is also approximately a medium size, $\omega^2 = 0.04$ [6].

In addition to evaluating the expectations of ability and motivation separately, a combined score was calculated to represent the general attitude. The score is represented as "positive" if a participant had positive expectations towards *both* ability and motivation (rating both as either "mostly" or "definitely" yes). The score is represented as "negative" if a participant had negative expectations towards *either* ability or motivation (rating at least one of the two factors either as "mostly" or "definitely" not). In all the rest of the cases, the score is represented as "neutral".

The reasoning behind computing the combined score is that both the ability and the motivation should be present in order for the service provider to act towards security and privacy protection; if either ability or motivation is lacking (e.g. if the service provider has the competence and resources to implement necessary protection, yet is willing to violate the privacy of its' users for the sake of better profits), the necessary protection measures will not be taken. The combined attitude score is shown on Figure 2. Figure 2 also shows that participants generally have more positive attitudes towards smart health devices compared to smart home devices.

4.2.2 Effect of Demographics. Additionally, we looked into the differences in participants' beliefs in the ability and motivation of smart system providers to protect their users based on their gender and age. These differences between the genders are shown on Figures 3b and 3a. As such, while there was little difference between the male and female

[3]The assumptions of the test, namely the independence of the responses and normal distribution of the data were met.

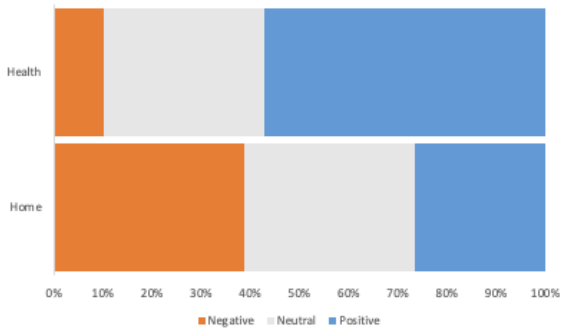
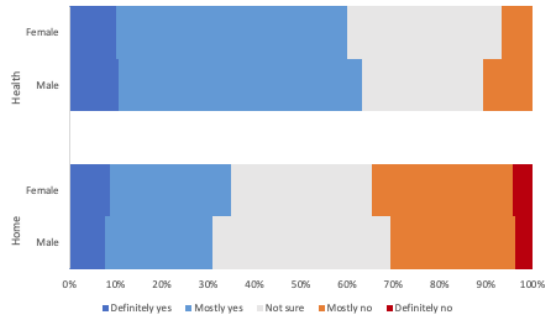
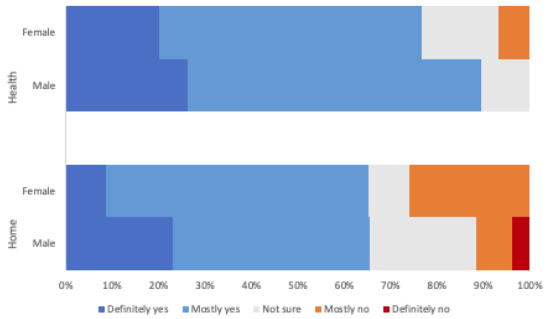


Fig. 2. Combined participants' attitudes towards ability and motivation of smart system providers to protect security and privacy of their users.

genders, slightly more women were either unsure or negatively inclined to believe the motivation of smart systems in both smart home and smart health groups. The statistical tests (one-way ANOVA), however, did not show any significant differences ($p > 0.05$).



(a) Participants' attitudes towards ability.



(b) Participants' attitudes towards motivation.

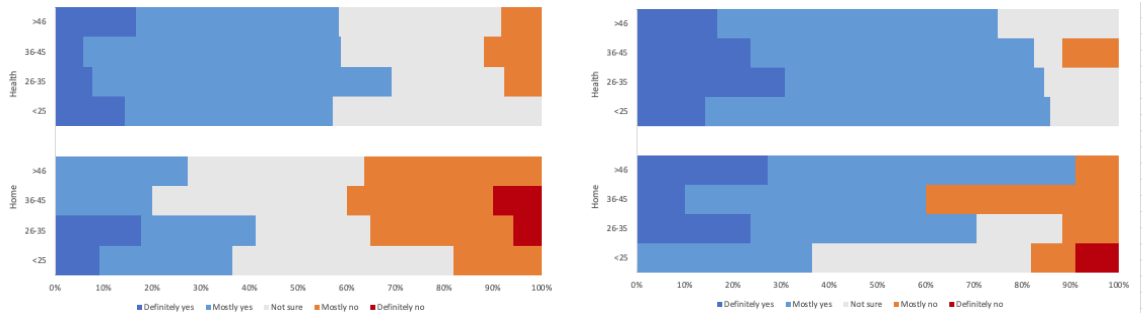
Fig. 3. Participants' attitudes towards ability and motivation by gender.

In a similar way considering participants' ages, when asked to consider the ability and motivation of smart home or smart health device providers to protect their security or privacy, although there were differences between the age groups, as can be seen in Figure 4, there was no significant deviation between participants[4]. It is worth noting however, that in the smart home group, more participants aged below 25 were "definitely" sure that providers were able to protect their privacy and security, Figure 4a, but also more convinced that these providers were less motivated to do so, as can be seen in Figure 4b.

4.3 Analysis of Free-Text Responses

The qualitative evaluation of the study was conducted via thematic analysis, identifying common themes as factors influencing the beliefs in either ability or motivation of smart system, i.e.: smart home and health device (system) providers. The analysis was performed by two authors of the paper. First, a list of broad categories, or factors, was

[4]Note, as several of the age groups had very few participants, we grouped them together in the figures.



(a) Participants attitudes towards ability.

(b) Participants attitudes towards motivation.

Fig. 4. Participants attitudes towards ability and motivation by age.

identified from a preliminary look at the data using an open coding approach, which was then discussed and further refined. The responses of each participant were then coded using the derived list of factors, and the results of the coding were discussed in several iterations in order to form an agreement. Finally, looking at the responses assigned to each factor, the themes within the factor were identified and analysed in order to gain a deeper understanding of what the factor meant to the participants.

4.3.1 Identified Factors. The analysis resulted in identifying the following seven broad factors: *security*, *privacy*, *financial issues*, *reputation*, *company profile*, *oversight* and *ethical issues*. The factors and the themes within them are discussed in further detail below.

Security. Many participants were concerned with the security or technology of smart devices and mentioned specific issues that they believed affected a provider's ability to protect their security or privacy. Mentions in this category fell into a number of broad subcategories, such as:

- *General negative attitudes.* Many participants believed that it is very hard or even impossible to protect security and privacy (e.g. "everything can be hacked").
- *General positive attitudes.* On the other hand, there were some beliefs in technology that can be used for protection (e.g. "technology is advanced enough") and held an overall positive view.
- *User's fault.* Another consistent trend was the human factor as a challenge in ensuring security, e.g. people choosing weak passwords or not configuring their system properly. This also included sentiments where participants felt companies did not bother with security because they knew that it was not a requirement of the users. This tendency to absolve companies of blame for security breaches was unexpected and usually framed in a negative light.
- *Specific technologies.* In addition to the more general attitudes towards security and privacy were several specific mentions of ways to protect security and privacy, such as encryption or two-factor authentication. Encryption was the most common technology mentioned and it was mentioned by 12.2% of respondents. The need for software and hardware updates and maintenance was also mentioned several times as a method of protecting users.
- *Attacks.* Participants mentioned attacks that were either general (e.g. "hackers") or, occasionally, more specific (e.g. "ransomware"). Hacking specifically was mentioned by 58.2% of participants, almost entirely in the context

of the ability of smart device providers to protect users. A number participants mentioned more specific viral attacks.

Privacy. In contrast to security, mentions relating to this factor focused on data privacy and access to personal data. Mentions in this category fell into a number of broad subcategories, such as:

- *Transparency about privacy policies.* Companies that provided information about how they use the collected data were seen as trustworthy, e.g. companies that assure their customers that their data is not sold on. On the other hand, privacy policies that were seen as too obscure or incomprehensible ("burying consent in Terms and Conditions") were seen as a red flag.
- *Unauthorised data access.* Data protection and storage was a large concern amongst participants. Participants specifically mentioned the danger of data breaches, hackers stealing data or companies actively re-purposing the data for other uses. For example, sharing or selling users' data without authorisation to third parties or using data collected for their own marketing objectives. In particular, the selling of their data to third parties for profit was a consistent concern amongst respondents.
- *User control.* Providing smart device users with the possibility to control their privacy settings, e.g. decide which data to share, was usually mentioned in conjunction with unauthorised access to data.
- *User's fault.* As with security, users are often seen as the ones who are at fault when their privacy is not protected, e.g. by choosing weak privacy settings. As before, this is a concerning trend as it seems users are seen to be to blame for not having control of their own data (even if it might not be possible).

Financial Issues. Financial issues were related to costs for the company or impact on paying customers. Mentions in this category fell into a number of broad subcategories, such as:

- *Costs of security and privacy measures.* A frequently mentioned theme was the cost of implementing security and privacy measures. In particular, the cost was named a significant factor for companies that do not have the necessary resources to invest in security and privacy, thus being unable to ensure proper security and privacy protection. Costs were also mentioned in context of companies preferring to invest their resources elsewhere (e.g. on development of new features), thus not prioritising users' security and privacy protection.
- *High value of data.* A further financial consideration that would prevent companies from taking proper security and privacy protection measures, was mentioned as the use of data as a source of profit for the company, either directly, through selling it, or indirectly, through using the data to train AI algorithms that provide better service and as a way to stay competitive. Furthermore, the high value of data was mentioned in the context of data breaches, as an additional incentive for potential attackers. As a counter-point, some participants mentioned that they see companies with different business models (e.g. one that mainly depends on selling products to customers rather than customer's data to third parties) as more likely to protect the privacy of customers.
- *Costs of data breaches.* A frequently mentioned positive factor in implementing security and privacy protection was the potential costs of data breaches that would otherwise occur. These costs include direct losses, e.g. in form of either fines by government or regulatory bodies, or returned devices, as well as customer losses if data breaches get publicised.
- *Customer's concerns.* Some answers mentioned customers' concerns underlying financial decisions by the companies when it came to security and privacy protection. As such, some participants expressed beliefs that that as users do not care about their privacy enough to be willing to pay more for privacy-friendlier solution, the

companies have no incentive to protect privacy of their users. Nonetheless, some of the participants did believe that companies take into account the users' willingness to pay for better security and privacy protection, and that these companies would implement the protection measures and use them as a selling point.

Reputation. The answers in this category mentioned some form of reliance on company's reputation when it comes to security and privacy protection. Mentions in this category fell into a number of broad subcategories, such as:

- *Name recognition and customer trust.* Commonly mentioned was the reliance on a company being an established brand in their field. Such brands, as some of the participants speculated, would have customers' confidence and trust, while on the contrary, companies who did not have the same level of recognition would be seen as someone who does have a lot to lose, hence, is not concerned about their reputation.
- *Company's track record.* Previous history of data breaches, or, conversely, of employing security and privacy practices, was seen as an important factor to elicit trust. While many answers mentioned that a history of security and privacy issues would be a negative sign for them, several mentioned that companies who experienced these issues might be both more knowledgeable in how to deal with them, and also more committed to fixing their mistakes.
- *Personal experience.* Some participants relied on their personal experience with using the system, seeing it as trustworthy as they have not experienced any problems with it so far. For some, this reasoning also extended to other products of the same company, thus increasing their trust in the system provider in general.
- *Media reports.* An important source of judging the trustworthiness of the system provider, mentioned by many participants, were media reports about security and privacy issues, including articles about data breaches or privacy violations. A lack of such reports and scandals was seen as a positive sign, while at the same time, these scandals did not only affect the perceived trustworthiness of the specific system affected. Consequently, reports about security and privacy of smart systems in general, such as publishing information about specific hacks, might affect the beliefs in the ability and motivation of such systems to protect one's security and privacy as well, even if a particular system has not been explicitly mentioned in such reports.
- *Word of mouth.* In addition to media reports and personal experience, learning about other users' experiences with the system was also mentioned as a way to judge the trustworthiness of the system. As such, sources of user feedback such as recommendations of family and friends, customer reviews and online communities were mentioned.

Company Profile. Participants also mentioned specifics about the smart system providers themselves. Mentions in this category fell into a number of broad subcategories, such as:

- *Company size.* There was a range of responses when it came to company size. Some participants believed that smaller companies were better at protecting their users than larger companies however many believed that larger companies had better resources to protect their uses (provided that they wanted to). The conflict here would indicate a lack of true awareness of which companies are good at this.
- *Company location.* The geographical location of the company was mentioned several times, with users contrasting Europe and America and regions where companies might not be able to avoid political or governmental interference. In general, companies that were able to distance themselves from governments or political parties were seen in a more positive light than ones that were government controlled. However, governmental links were seen as a positive, in terms of oversight, for smart health devices.

- *Company branding.* Answers in this category included mentions of the size of the brand, its experience and specific company names. Of the companies mentioned, Apple (including mentions of Siri), Amazon (including Alexa and Ring) and Google (including Google Assistant and Nest) were the companies mentioned the most, comprising 71.9% of total mentions of company names. In terms of unique users, 39.3% users mentioned Amazon, 19.1% mentioned Google and 13.5% mentioned Apple. The majority of mentions of Google and Apple were positive, however the mentions of Amazon were mostly in a negative context. Much of this negative opinion was attributed to Amazon's Alexa voice activated virtual assistant. A lot of user opinions were swayed by company branding which may be biasing their opinions.

Oversight. Oversight was defined as any mention where the participant felt that a third party did, or should, oversee smart system providers in some capacity. Mentions in this category fell into a number of broad subcategories, such as:

- *Legislation.* Legislation was often named as a driving factor in ensuring proper security and privacy protection, either through holding companies accountable, via fines and other kinds of consequences, or by not allowing products to operate without proper user protection. In particular, the responses mentioned both the role of appropriate legislation in general, as well as legislation in specific geographic domains such as Europe, in particular, mentioning the GDPR[5]. At the same time, lack of proper legislation, or its insufficient responses, was mentioned as a factor that kept companies from implementing security and privacy measures by failing to incentivise them in a sufficient way.
- *Governmental oversight.* In addition to legislation, other ways for governments to oversee that companies implement proper security and privacy protection measures were mentioned. These include forms of governmental investment in the company (e.g. as governmental grants), use of a particular smart system as a part of governmental services (e.g. the NHS) or government control in general. On the other hand, involvement by the government was also mentioned as a negative factor by some of the participants by implying e.g. that the government might demand access to customer data from the company, thus leading to privacy issues.
- *Independent verification.* A further form of oversight mentioned by participants consisted of different kinds of independent verification of the security and privacy protection in the system, which was not necessarily government-mandated. Such verification, in particular, was mentioned in form of expert reviews of the system, certification obtained by the company or as a general reference to relying either on a trusted third party or other means to prove the provider's claims.

Ethical Issues. The responses in this category referred to the intrinsic motivation of the system providers to protect the security and privacy of their users. As such, the participants believed that companies should have an ethical responsibility towards their users. Hence, having integrity and caring about their users was mentioned as a factor in whether system providers ensure the necessary security and privacy protection.

4.3.2 Frequency Analysis. When counting the number of distinct factors mentioned by each participant (out of the aforementioned seven), more than half of the participants (52 out of 98) mentioned at least five factors. Furthermore, the number of participants who mentioned each one of the aforementioned factors was counted. The frequency analysis of the identified factors is shown in Figure 5. This is broken down by group, smart health or smart home in Figure 6. It can be seen in Figure 5 that security factors were mentioned most commonly in the context of the ability of smart

[5]Note also that although the study was performed among the UK participants, it took place shortly before Brexit was finalised, with the UK still formally being a part of EU.

device providers to protect users' security and privacy while financial factors were mentioned more commonly in the context of the motivations of smart device providers to protect users' security and privacy. When looking at the smart home and smart health groups separately, as shown in Figure 6, it can be seen that while broadly speaking most factors were mentioned equally by participants in both groups, reputation, privacy and oversight factors were mentioned more frequently by the smart health group.

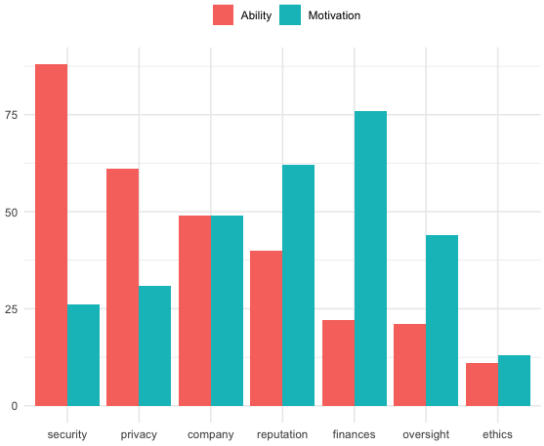


Fig. 5. Number of participants mentioning each factor as influencing their beliefs either in ability or motivation (sorted by factors most commonly mentioned for ability).

Fig. 6. Number of participants in smart health and smart home groups mentioning each factor (sorted by factors most commonly mentioned in both groups).

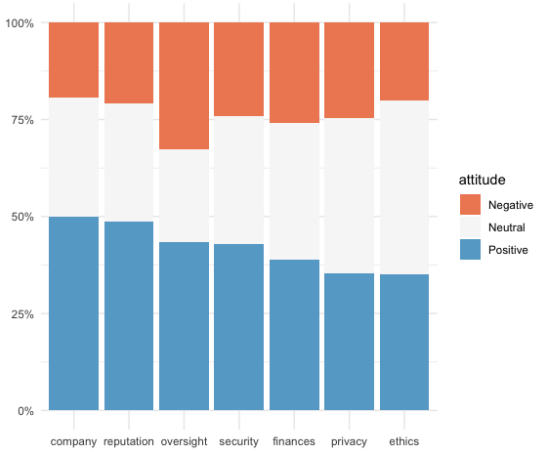


Fig. 7. Distribution of attitudes within participants mentioning each factor (sorted by factors mentioned by the highest fraction of participants with a positive attitude).

Fig. 8. Correlation between participants mentioning each pair pair of factors.

Figure 7 summarises the distribution of participants with positive, negative or neutral attitudes among the ones who mentioned each factor. It can be seen that participants had a broadly positive attitude towards all factors, although oversight was the most likely to be mentioned by participants who had a negative attitude towards the smart systems.

Finally, Figure 8 shows the correlation between the factors being named, with only significant ($p < 0.05$) correlations being displayed[6]. It can be seen here that there are a number of positive correlations. The factors most likely to be mentioned together include finances and reputation (e.g. as losing profits due to losing customers because of bad press), oversight and privacy (e.g, mentioning compliance to privacy-related regulations), oversight and company profile and oversight and reputation.

5 DISCUSSION

The results are discussed here and recommendations on how to improve trust in smart systems are proposed.

5.1 Limitations

The study suffers from the limitations common to online surveys: as such, while we were able to get valuable insights from the participants of our survey, the format of the survey did not allow us to ask follow-up questions for clarification or more in-depth investigation. Furthermore, the majority of the participants in our sample had experience with using smart systems, perhaps leading to them to being, or believing that they were, more knowledgeable about these systems than the general population.

5.2 Implications of Results

There are a number of overall trends that can be seen from the results.

Although there is no marked difference between participants responses when it came to gender or age, there was a clear difference in overall attitudes and responses between participants in the smart health and smart home groups. Participants believed that smart home device providers were less able to protect their users' security and privacy than smart home providers. Participants also believed that although both smart home and smart health device providers were overall motivated to protect their users' security and privacy, smart home device providers were less motivated to do so than smart health providers.

Part of this division can be explained by examining the participants free text answers. In particular the factor analysis showed that most participants mentioned financial factors as a motivation for protecting users security and privacy while security factors were most mentioned when it came to smart device (system) provider's ability to protect users. There was a common trend that due to the type of data that smart health devices collect, some participants believed these providers were more stringently regulated or would suffer from legal or financial repercussions if there was a privacy or security breach. This theme was less explicit in the responses regarding smart home devices, as was also evidenced from the difference in number of participants who mentioned the "oversight" factor in smart home and smart health groups. At the same time, more participants mentioned potential privacy issues for smart health than smart home systems, while mentioning more security concerns, where privacy and unauthorised access to data, for smart home systems. This may be due to participants recognising that health data was more sensitive or perhaps due to not having a clear understanding of what data smart home systems might have access to. Many participants also drew

[6] Analysis conducted using the R "stats" package.

distinctions between high and low value data, in terms of it being sold or re-purposed for other uses like marketing, but did not qualify what this data might be.

This lack of awareness prevailed overall. There was a trend amongst all participants of being unsure whether companies could and would be able to protect users' security and privacy. This was despite their exposure to smart devices already (most participants had used a smart device previously and the majority indicated they wanted to do so in the future). Many participants based their judgements off of news articles or company branding, and showed little awareness of the specifics of how smart home or health devices collected data and how it was regulated, they frequently outsourced their thinking to "experts" or "legislation" who would protect them from companies' misusing their data.

A particularly concerning trend was that many people absolved companies of blame and blamed each other instead. For example either explicitly blaming other users for their own security failures, setting poor passwords, or implicitly blaming other users for not caring about their security or privacy and therefore the companies do not have to care either as it is not a user requirement in order to sell devices. No respondents took personal blame for making any of these mistakes or made suggestions for their own improvement. They tended to blamed others for faults or human errors which in turn negatively impacted the participant in question.

Generally, the participants mentioned a variety of factors influencing their beliefs regarding the ability and motivation of smart systems. This shows not only that providing information about the system would be helpful towards ensuring trust, but also that this trust relies on multidimensional aspects, each of them is important to gain confidence of the end users.

5.3 Recommendations

Following on from these trends there are a number of recommendations which should be taken on board when designing systems such as smart home or smart health devices (systems).

5.3.1 Transparency. As the responses mentioned different kinds of information the participants would find helpful, providing such information to the users would be a step towards ensuring better transparency. Yet, in order to avoid overwhelming the user, provide the most important information in a simple to understand form, while at the same time also providing the users with access to more detailed information in case they want to find out about further details.

5.3.2 User controls. As many users mentioned the importance of having control over their data, proper security and privacy settings should be implemented in smart systems. The users should be able to have access to the desired functionality even without sharing their data or otherwise making their system vulnerable e.g. by leaving it constantly connected to the internet. On the other hand, one needs to avoid making the controls too complicated; if needed, provide only the most important options to the user (ideally, implementing privacy by default), while letting them have access to more fine-grained options if they want to. One potential way to do this could be by using a collective action based mechanism to address user concerns as proposed by Flouris et al.[7] which would allow users' to communicate their security and privacy preferences to each other.

5.3.3 Accountability. Companies should be open about accountability measures they comply with. Additionally, the society (policy makers and the general public) should ensure that companies face consequences by (1) enforcing compliance to legislation, (2) making sure that improper practices are exposed and publicised, (3) raising awareness among the public.

5.3.4 Developer education. Given the complexity of proper security and privacy protection in general, as well as cases where security and privacy are not prioritised (e.g. due to focus on functionality or lack of resources and expertise within the company), lack of awareness about security and privacy among the developers might become an issue, especially for smaller companies. Ensuring that developers have a proper understanding both of technical challenges in ensuring security and privacy, as well as in ethical issues of data protection, is therefore of great importance. Considering ethics in system design in particular, is something that has previously been mentioned[18] as a way to protect end users' privacy and security.

5.3.5 User education. As many recognise the role user behaviour plays in ensuring security and privacy, there should be an accessible way for the users to learn secure and privacy-preserving behaviour. At the same time, it is important not to shift too much responsibility on the users, recognising that the primary responsibility is on the companies.

6 CONCLUSION

In this paper a mixed methods online study of smart system, specifically smart home and smart health devices, was presented. The main aim of the study was to investigate the factors that influence end users' trust in the security and privacy protection of smart systems, in particular, the extent to which the users perceive the ability and the motivation of system providers to ensure the necessary protection. To this end, the results of the study were presented and based on the conclusions draw from participants' responses a number of recommendations were proposed. These recommendations should be taken into account by smart system providers when designing such systems in order to increase end users' trust.

Security and privacy issues are seen as one of the grand challenges for HCI research in the future[21]. This paper goes towards proposing ways in which end user trust in future technology, like smart systems, can be improved. Many of the recommendations made in this paper revolve around how information is relayed to end users, for example, when it comes to ensuring transparency and accountability. Fundamentally end users are often not aware of how little they know about a particular company or smart system. Even when questioned, they are unaware of their lack of knowledge. As a result they have to rely on potentially biased or flawed information when it comes to making decisions about which systems to trust -including blaming each other for the behaviour of an essentially faceless company. Providing end users accurate and honest information, in a way they can understand it, and coupling this with allowing users to control their data is the best way to enhance users' trust in a system.

While the study had an exploratory nature, future work would focus on more in-depth investigation of its findings. As such, the relative importance of the identified factors could be studied in different contexts and within different demographics (including cross-cultural studies) as well as different ways to convey the information about these factors.

ACKNOWLEDGMENTS

This work was partially funded by the European Unions Horizon 2020 Research and Innovation Programme through the GHOST project (https://www.ghost-iot.eu/) under Grant Agreement No. 740923.

REFERENCES

[1] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 137–153.

[2] Alessandro Acquisti. 2009. Nudging privacy: The behavioral economics of personal information. *IEEE security & privacy* 7, 6 (2009), 82–85.

[3] Louise Barkhuus. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 367–376.
[4] Christy Cheung and Matthew KO Lee. 2000. Trust in Internet shopping: A proposed model and measurement instrument. *AMCIS 2000 Proceedings* (2000), 406.
[5] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.
[6] Andy Field. 2018. *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). SAGE Publications Inc. 1071 pages.
[7] Giorgos Flouris, Theodore Patkos, Ioannis Chrysakis, Ioulia Konstantinou, Nikolay Nikolov, Panagiotis Papadakos, Jeremy Pitt, Dumitru Roman, Alexandru Stan, and Chrysostomos Zeginis. 2018. Towards a Collective Awareness Platform for Privacy Concerns and Expectations. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* 11229 LNCS (2018), 135–152. https://doi.org/10.1007/978-3-030-02610-3_8
[8] Radhika Garg. 2019. An Analysis of (Non-)Use Practices and Decisions of Internet of Things. In *Human-Computer Interaction – INTERACT 2019*, David Lamas, Fernando Loizides, Lennart Nacke, Helen Petrie, Marco Winckler, and Panayiotis Zaphiris (Eds.). Springer International Publishing, Cham, 3–24.
[9] David Gefen, Elena Karahanna, and Detmar W Straub. 2003. Trust and TAM in online shopping: An integrated model. *MIS quarterly* 27, 1 (2003), 51–90.
[10] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, and Michael H. Breitner. 2020. Privacy concerns in the smart home context. *SN Applied Sciences* 2, 2 (2020), 247.
[11] Sabrina Karwatzki, Manuel Trenz, Virpi Kristiina Tuunainen, and Daniel Veit. 2017. Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems* (2017), 688–715.
[12] Oksana Kulyk, Paul Gerber, Michael El Hanafi, Benjamin Reinheimer, Karen Renaud, and Melanie Volkamer. 2016. Encouraging privacy-aware smartphone app installation: Finding out what the technically-adept do. (2016).
[13] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. this website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC)*.
[14] Oksana Kulyk, Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Nina Gerber, and Melanie Volkamer. 2020. Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation. In *Financial Cryptography and Data Security Workshop on Usable Security (AsiaUSEC), February 14, 2020 Sabah, Malaysia*. Springer.
[15] Alexander Kunst. 2020. Smart home device ownership in the UK 2020. https://www.statista.com/forecasts/997845/smart-home-device-ownership-in-the-uk#statisticContainer
[16] Edith Law, Krzysztof Z Gajos, Andrea Wiggins, Mary L Gray, and Alex Williams. 2017. Crowdsourcing as a tool for research: Implications of uncertainty. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 1544–1561.
[17] Helen Nissenbaum. 2004. Will Security Enhance Trust online, or supplant it? *Trust and Distrust Within Organizations: Emerging Perspectives, Enduring Questions, Eds. R. Kramer and K. Cook, Russell Sage Publications (2004)* (2004), 155–188.
[18] Jeremy Pitt. 2012. Design Contractualism for Pervasive / Affective Computing. *Technol. Soc. Mag. IEEE* 31, 4 (2012), 22–29. http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=6387955
[19] Jens Riegelsberger, M Angela Sasse, and John D McCarthy. 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies* 62, 3 (2005), 381–422.
[20] Michael Warren Skirpan, Tom Yeh, and Casey Fiesler. 2018. What's at Stake: Characterizing Risk Perceptions of Emerging Technologies. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, Article 70, 12 pages.
[21] Constantine Stephanidis, Gavriel Salvendy, Margherita Antona, Jessie Y.C. Chen, Jianming Dong, Vincent G. Duffy, Xiaowen Fang, Cali Fidopiastis, Gino Fragomeni, Limin Paul Fu, Yinni Guo, Don Harris, Andri Ioannou, Kyeong ah (Kate) Jeong, Shin'ichi Konomi, Heidi Krömker, Masaaki Kurosu, James R. Lewis, Aaron Marcus, Gabriele Meiselwitz, Abbas Moallem, Hirohiko Mori, Fiona Fui-Hoon Nah, Stavroula Ntoa, Pei Luen Patrick Rau, Dylan Schmorrow, Keng Siau, Norbert Streitz, Wentao Wang, Sakae Yamamoto, Panayiotis Zaphiris, and Jia Zhou. 2019. Seven HCI Grand Challenges. *Int. J. Hum. Comput. Interact.* 35, 14 (2019), 1229–1269. https://doi.org/10.1080/10447318.2019.1619259
[22] Melanie Volkamer, Karen Renaud, Oksana Kulyk, and Sinem Emeröz. 2015. A socio-technical investigation into smartphone security. In *International Workshop on Security and Trust Management*. Springer, 265–273.
[23] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 65–80.

A INFORMATION ABOUT SMART SYSTEMS

A.1 Smart Home

A smart home refers to a household in which household appliances (e.g. refrigerator, washing machine, vacuum cleaner), household automation devices (e.g. heating, lighting, ventilation) and entertainment electronics or communication

devices (e.g. TV, game consoles) are connected and become "intelligent" objects. By connecting these and combining several such items, new functions and services become possible that offer added value over the individual item. The objects can be controlled centrally from the smart home or remotely via the internet (e.g. through a voice assistant).

Smart home system providers refer to entities that are involved in either design and development, implementation, deployment and maintaining of the smart home systems. Such entities can be governmental agencies, non-government organisations or private companies.

A.2 Smart Health

Smart Health describes electronic-based diagnosis and treatment systems (e.g. blood pressure monitors, scales, thermometers), special sensors (e.g. fall sensors, sensors in the toilet, heat sensors), wearables (e.g. smart watches, fitness trackers or smartphones) up to intelligent body modifications (e.g. implants or prostheses) which are connected to each other. By networking these and combining several such items, new functions and services become possible that offer added value over the individual item. The diagnostic/treatment/sensor devices can often be connected to another device, e.g. wearables or smartphones, and thus additionally controlled.

Smart health system providers refer to entities that are involved in either design and development, implementation, deployment and maintaining of the smart home systems. Such entities can be governmental agencies, non-government organisations or private companies.

B QUESTIONNAIRE

(1) What is your personal experience with using smart health devices?
   - I often use smart [home/health] devices
   - I sometimes use smart [home/health] devices
   - I used smart [home/health] devices in the past, but do not do it anymore
   - I never used a smart [home/health] device.

(2) If you are not currently using a smart [home/health] device, would you like to use them in the future?
   - Yes
   - No

(3) Do you believe smart [home/health] system providers can protect the security and privacy of their users?
   - Definitely yes
   - Mostly yes
   - Not sure
   - Mostly no
   - Definitely no

(4) Please explain your answer

(5) What factors would influence your beliefs (e.g. which information about specific system or specific system provider would make you feel either more or less confident regarding their capability)? You can name more than one factor.

(6) In your opinion, are there any differences in the capability of smart [home/health] system providers to protect the security of their users and their capability to protect the privacy of their users?
   - Yes, namely:
   - No

- Not sure

(7) What do you believe are the most significant challenges the smart [home/health] system providers face in protecting the security and privacy of their users? You can name more than one challenge.
(8) In your opinion, which kind of smart [home/health] system providers are most capable of protecting the security and privacy of their users?
(9) In your opinion, which kind of smart [home/health] system providers are LEAST capable of protecting the security and privacy of their users?
(10) Do you believe that smart [home/health] system providers are motivated to protect the security and privacy of their users?
    - Definitely yes
    - Mostly yes
    - Not sure
    - Mostly no
    - Definitely no
(11) Please explain your answer
(12) What factors would influence your beliefs (e.g. which information about specific system or specific system provider would make you feel either more or less confident regarding their motivation)? You can name more than one factor.
(13) In your opinion, are there any differences between the motivation of smart [home/health] system providers to protect the security of their users and their motivation to protect the privacy of their users?
    - Yes, namely:
    - No
    - Not sure
(14) What do you believe are the most significant factors that could motivate the smart [home/health] system providers in protecting the security and privacy of their users? You can name more than one factor.
(15) What do you believe are the most significant factors that would make the smart [home/health] system providers LESS motivated to protect the security and privacy of their users? You can name more than one factor.
(16) In your opinion, which kind of smart [home/health] system providers are most motivated of protecting the security and privacy of their users?
(17) In your opinion, which kind of smart [home/health] system providers are LEAST motivated of protecting the security and privacy of their users?