Exploring Consumers' Attitudes of Smart TV Related Privacy Risks

Marco Ghiglieri[1], Melanie Volkamer[1,2], and Karen Renaud[3]

[1] Technische Unviersität Darmstadt, Darmstadt, Germany
marco.ghiglieri@crisp-da.de,
[2] Karlstadt University, Karlstad, Sweden
[3] University of Glasgow & Mississippi State University

Abstract. A number of privacy risks are inherent in the Smart TV ecosystem. It is likely that many consumers are unaware of these privacy risks. Alternatively, they might be aware but consider the privacy risks acceptable. In order to explore this, we carried out an online survey with 200 participants to determine whether consumers were aware of Smart TV related privacy risks. The responses revealed a meagre level of awareness. We also explored consumers' attitudes towards specific Smart TV related privacy risks.
We isolated a number of factors that influenced rankings and used these to develop awareness-raising messages. We tested these messages in an online survey with 155 participants. The main finding was that participants were generally unwilling to disconnect their Smart TVs from the Internet because they valued the Smart TV's Internet functionality more than their privacy. We subsequently evaluated the awareness-raising messages in a second survey with 169 participants, framing the question differently. We asked participants to choose between five different Smart TV Internet connection options, two of which retained functionality but entailed expending time and/or effort to preserve privacy.

Keywords: Smart TV, Privacy, Risks, Human Factors, Consequences

1 Introduction

Smart TVs are a relatively recent innovation that, in addition to streaming traditional broadcast content, facilitate access to Internet content and services as well as video-on-demand, games and infotainment. At first glance, Smart TVs seem to deliver distinct added value, as compared to traditional televisions. A closer look reveals a number of privacy risks in the Smart TV ecosystem: (1) vendors and broadcasters routinely collect and share Smart TV usage-related data [45,19,15], (2) many vendors record and analyze speech by transmitting it to third party services to extract commands for operating the TV [26] and (3) Smart TVs are less reliably secured than desktop computers and smartphones, [27]. In effect, consumers connecting their Smart TVs to the Internet are, perhaps unwittingly, sacrificing their privacy. There seems to be little pressure from

consumers to force vendors and broadcasters to respect their privacy. Two explanations are possible: (1) consumers are unaware of the privacy risks and/or (2) consumers are aware of the risks but consider them acceptable or too unlikely to be concerned about.

The primary aim of our research was first to assess general awareness of these privacy risks. We discovered a poor level of awareness, so we proceeded to develop strategies to improve consumer awareness and also to explore the likelihood that consumers would be prepared to act to protect their privacy. Our research project's phases were as follows:

First, we explored general levels of consumer awareness of risks using an online survey. This included understanding which particular risks were considered critical, and why. This online study with 200 participants confirmed a low level of general awareness. From the participant responses we derived factors that clearly influenced participants' risk judgments. We then used these factors to craft effective awareness messages to be used in phase two.

Second, using an iterative approach, we developed two awareness messages based on the factors we isolated during the first phase, and evaluated them. One message raised awareness of usage data collection and analysis. The other did this, but also flagged the possibility of their usage data being misused. We conducted an online study with 155 participants to test the impact of these messages, as measured by their willingness to disconnect their Smart TVs from the Internet. Most participants were unwilling to do this. The most commonly-mentioned reason for this was the fact that they wanted to retain the Smart TV's Internet functionality. Even though we increased awareness of privacy risks, they valued the Internet functionality so much that the risks did not seem to concern them.

Third, we tested whether privacy-aware consumers would be willing to spend time and/or money in order to preserve their privacy, all the while retaining the TV's Internet functionality. We presented participants with a privacy-protection mechanism such as the one proposed by Ghiglieri *et al.* [19]. This mechanism installs broadcaster and vendor privacy protection before the Smart TV is connected to the Internet. Internet functionality is unhindered but the consumer's privacy risk is reduced. 169 people participated in a study to explore reactions to, and acceptability of, this mechanism. Most participants declared themselves willing to deploy this kind of privacy-protection mechanism.

Our main findings are as follows:

- We confirmed a generally low level of awareness of privacy-related risks in the Smart TV context.
- Some participants were aware that data was being gathered and analyzed, but unaware of the potential for misuse.
- Making participants aware of potential misuse is more effective than only making them aware that data is collected and analyzed by vendors (whom they may trust).

– Raising awareness, in and of itself, is insufficient. Together with awareness, people also need the means to preserve their privacy.
– Expecting people to forego all Internet functionality is unrealistic. However, they express a willingness to spend time and/or money on privacy protection as long as they can retain Internet functionality.

In conclusion, it is clear that research into the development of usable privacy enhancing technologies (PET), providing an improved level of privacy preservation while retaining functionality, is required. Awareness-raising, on its own, is insufficient.

2 Background

Publications and media have shown that Smart TV consumers are exposed to privacy risks such as the collection and analysis of usage data for various purposes. A blog [9] revealed that the privacy policy of LG contains a corresponding statement; Samsung's [34] and Sony's [37] privacy policies also contain such statements. Furthermore, published studies [18,19,16,14] showed that the Internet functionality HbbTV has been also used to profile consumers without consumer's consent. HbbTV is a standardized technique that covers video-on-demand and information services for Smart TVs provided by the broadcasters. It is supported by 97% of the current available Smart TVs [35], in Germany, the country in which this research was conducted. According to the Smart TV working group of the German TV-Platform [1] a worldwide usage of HbbTV is being contemplated. Europe has the highest coverage as of today. Other publications have shown that even the (traditional) broadcast channel of the TV signal is vulnerable and can be manipulated so that it can transport malicious data to Smart TVs in a specific regional area (e.g. manipulating HbbTV in Oren *et al.* [30]). Furthermore, Michéle *et al.* [27] showed that Smart TV media players could enable TV hacking and allow secret access to camera and microphone data streams. Indeed, in Metro [33], a news paper, it was reported that a couple was recorded in an intimate situation by hackers. The recorded video was published. More vulnerabilities have been revealed: Smart TV Apps [28], Vendor transferred voice data unencrypted [5] and incorrect implementation of HTTPS certificate validation [17].

3 Methodology — Consumer Awareness

We describe the study design, recruitment and ethics as well as the methodology for the evaluation of the free text answers for the online survey to explore levels of consumer awareness of risks.

3.1 Study Design

It comprised the following steps (see Figure 1):
Welcome and introduction. First, participants were informed that the survey

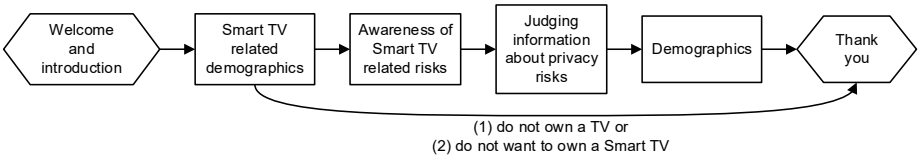

Fig. 1. Study Design.

focused on Smart TVs. They were not briefed about the exact focus of the survey so as not to prime their responses. Information about the duration was provided, as well as the fact that there were no wrong answers.

Smart TV related demographics. Participants were asked whether they owned a TV. Those who did were informed what a Smart TV is and asked whether their own TV was smart. Those who did not own a Smart TV were asked whether they would like to own one. Only those who owned a Smart TV, or wanted to own one, continued. The remaining participants were forwarded to the "Thank you" page.

Awareness of Smart TV related risks: Participants were asked to enumerate Smart TV risks they are aware of. Afterwards, they could name measures that could be used to counteract these risks.

Judging information about privacy risks. Participants were given four different risks to contemplate, one per page, in random order. For each, participants were asked to judge how critical it was. Options for the rating ranged from 1 'not very critical' to 3 'neutral' to 5 'very critical'. The option 'don't know' was also available. They were asked to justify their ratings. The request for justification appeared on the same page as the scenario description.

The displayed privacy risks were identified from the research literature and public media (see Section 2). The following scenarios were presented to the participants (we add one reference as an example reference for further information about the corresponding attack):

- **Broadcaster Profiling.** The TV gathers information about how long, and how often, you watch each channel. If the broadcaster offers multiple channels, it is possible that the usage information from different channels is aggregated (see e.g. [14]).
- **Vendor Profiling.** The Smart TV vendor gathers information about how you use the TV. For example, the vendor gets detailed information about which apps you use. Furthermore, it gathers information about how long, and how often, you use your TV (see e.g. [45]).
- **Voice Recognition.** If you decide to control your Smart TV with your voice, anything you say is transmitted to, and analysed, by the vendor's servers. To provide this functionality, it is necessary to transmit all utterances in the room, for processing by the vendor's servers (see e.g. [26]).
- **Surveillance Audio.** Your Smart TV is equipped with a microphone. Outsiders can gain access to the Smart TV and are able to activate it and listen

to all the conversations in your living room. You do not realize this (see e.g. [27]).

Demographics. Participants were asked to provide information about gender and age.
Thank you. Finally, we thanked participants for their support and they received information on how to claim their monetary reward.

3.2 Recruitment

The study was conducted in Germany in December 2015. SoSciSurvey[4] was used as platform for the survey. The participants were recruited via clickworker[5] which is similar to Amazon Mechanical Turk but recruits in Germany instead of the USA. We paid each participant who completed the survey, and did not provide obvious nonsense answers, €2 per participant on that platform.. We measured the average time with test participants. This was about twelve minutes. As Germany has a minimum wage of €8.50 per hour €2 was fair payment.

3.3 Ethics

Guidelines on ethical issues regarding research involving humans are provided by the host university. These guidelines were followed with respect to respondent consent and data privacy requirements were met. Participants first read an information page on which they were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, using SoSciSurvey ensured that data was stored in Germany and thus subject to German data protection law. They were told that they could withdraw at any time. Moreover, they were told that all answers were valid: there was no such thing as a wrong answer. No debriefing was required.

3.4 Evaluation Methodology

We used open coding to analyze free text answers. We proceeded in the following way: First, two authors analyzed the free text answers independently and composed a list of codes. Furthermore, they clustered these codes in categories. Afterwards, the categories were discussed and the authors agreed on one list of categories as well as a mapping from code to category. These categories were afterwards applied to the free text answers by two authors. Then, the assignments were compared and discussed to agree on the categories to be assigned. It was possible to assign one answer to several categories.

Note, all studies were conducted in Germany and questions and quotes in German were translated for inclusion in this paper.

[4] `http://www.soscisurvey.de`
[5] `http://www.clickworker.com/`

4 Results — Consumer Awareness

4.1 Sample

200 participants completed the survey. 8 were removed from the data set since they entered implausible values (e.g. data and rating did not match, empty free text fields all over the place). The survey group consisted of 104 females (54%) and 87 males (45%); 1 (1%) did not provide gender. The youngest participant was 19, the oldest 89 and the mean age was 38.9 years with a standard deviation of 12.41.

14 participants (7%) indicated that they did not own a TV. Out of the 178 remaining participants who owned a TV, 127 (71%) have a Smart TV and 51 (29%) owned a non-Smart TV. 44 (86 %) of those who did not own a Smart TV would like to have one but 7 (14%) did not. 171 participants completed the survey with the questions about the scenarios.

4.2 Awareness of Risks

We assessed whether participants knew about Smart TV privacy risks. In total, 60 individual text fields for risks were cited. The average number of risks per participant was 2.14 for those who mentioned at least one risk; overall 0.16. 28 (16%) participants mentioned at least one risk; 11 (11%) of the female participants who were asked to mention risks mentioned at least one.

We analyzed the 60 free text risk-related responses in terms of two aspects: 'potential actions' or 'consequences' of a risk. The most often mentioned potential action was 'collecting data' (19 participants), 'access to camera or microphone' (17). The other categories are 'access to sensitive data' (4), 'access to network' (3), and 'TV manipulations'. These aspects were mentioned by 21 participants. The most often mentioned consequences of privacy risks are 'personalized advertising' (7) and 'being robbed' (3). The others are: 'TV getting too slow' (2), 'Child watches inappropriate content' (2), 'TV does not work' (2) and 'program could change' (1). These consequences were mentioned by 12 participants.

We confirmed a general lack of awareness of privacy risks, and concrete consequences thereof.

4.3 Risk Scenario Ratings

We analyzed how critical participants rated the displayed privacy risk scenarios. Table 1 provides, for each scenario, (1) the number of participants who answered 'I don't know', (2) the number of participants considered[6], (3) the mean value how critical the scenario is rated for all participants, all female/male participants, as well as those mentioning/not mentioning risks in the previous part of

[6] Note, the total numbers differ as the number of people who answered 'I don't know' may differ as well as those who were set to 'not using' differs from scenario to scenario.

the survey. The 'broadcaster profiling' scenario was considered by most of the participants as the less critical one (light gray) and the 'surveillance audio' one as the most critical one (dark gray).

Table 1. How critical a scenario is rated for different subgroups of participants and different scenarios. (available options were: from 1 'not very critical' to 3 'neutral' to 5 'very 'critical'; and the option 'don't know' was available; most critical is filled dark gray and least critical light gray.)

Scenario	**I don't know**	**all**	**female**	**male**	**Risks**	**No Risks**
Broadcaster Profiling	4	2.82 (164)	2.66 (95)	3.06 (68)	3.19 (27)	2.74 (137)
Vendor Profiling	2	3.46 (168)	3.52 (95)	3.42 (72)	3.50 (28)	3.45 (140)
Voice Recognition	10	3.97 (159)	3.99 (91)	4.00 (67)	4.07 (27)	3.95 (132)
Surveillance Audio	4	4.69 (166)	4.75 (95)	4.67 (70)	4.64 (28)	4.70 (138)
$\sum$	20	3.74 (657)	3.73 (376)	3.79 (277)	3.85 (110)	3.71 (547)

4.4 Influencing Factors

In total 684 free text answers for the justifications, with more than 7,200 words, were examined using an open coding approach. We identified the factors that potentially impact the ratings related to privacy risks. The different factors are explored in the following paragraphs:

Party who gathers the data is likely to be an influential factor because many participants consider vendors and broadcasters collecting data to be acceptable: e.g. "*Vendor may take the data as long as there is no abuse*", "*I consider broadcasters to be secure*". However, criminals would use data to harm them ("*On top of that there is a danger of data being abused by criminals*").

The **type of data** is also likely to be an influential factor. Some participants were not worried about the described privacy risk as they considered the addressed usage data to be unimportant, i.e. not worth protecting as compared to other types of data: "*Don't care about usage data*", "*Inspection of usage data is relatively uncritical as long as there is no inspection of personal data such as Skype conversations*", "*Don't mind as long as they don't have access to personal data such as passwords or banking details*", "*Inspection of usage data seems uncritical*","*I don't care about usage data*", "*The danger of abuse is minimal*",

"*Information about my usage behaviour can be passed on*".

Being aware that usage data collection constitutes a privacy risk might have an influence. Some participants see no disadvantages ("*There is no disadvantage for me", "I think it has no negative effects on me*") or only consider the advantages to vendors and broadcasters of collecting and analyzing usage data:

- More reliable viewing figures: "*At least better than faked viewing figures*", "[..] *I don't really like it, but, on the other hand, it would be a real improvement in viewing figures*"
- Better products: "*Usage data is required in order to improve products*", "*It is important to support future development, because you can see which applications are used frequently and which not*".

On the other hand, other participants consider any collection of (usage) data a privacy invasion ("*I totally decline any data-gathering*", "*violates my privacy*", "*very bad, would violate my privacy a lot. If this happened,I would not feel very comfortable*".) as well as with terms like surveillance ("*I don't want to be kept under surveillance*") and profiling ("*you can create a user profile*").

Even when they are aware of a privacy risk, **being aware of possible misuses** might have an influence. Those who are aware of possible misuse mentioned different types of misuse:

- Vendors generally misuse the data: "*data can be abused*", "*my voice could be used without my knowledge*". Note, the last quote actually addresses an interesting aspect: '*without my knowledge*'. However, this aspect was only mentioned very rarely.
- Vendors sell data: "*It is critical; I don't want the vendor to sell my data. It is a private affair*".
- Burglary: "*It invades definitely my privacy, no one may want that. Burglars can check if someone is at home or not. If yes, they can burglarize or check if burglary would be worth at all on the basis of information obtained . If that isn't critical enough, I don't know...*".
- Close a Deal: "*With my voice someone could fake phone calls to confirm orders or contracts. In addition, there is a risk that not only commands to the Smart TV are recorded, but also private or business conversations are recorded*".
- Espionage: "*I would feel spied on*", "*It isn't ok if I, as a customer, am spied on in this way. The legislature must do something*".

Most of these were only mentioned by one or two participants.

Considering **personalized advertising as beneficial** or **irritating** seems to be an influencing factor:

- Some like personalized advertising since it suggests items of interest: "*I'll benefit from the analysis of my usage behaviour as they provide me with tailored advertisements and special programmes for me personally*".

– Others consider this to be a nebulous attempt to misuse their data: "*Could be evaluated for personalized advertisement and programs -¿ data may be sold to other companies in the media group*".

People's **general privacy attitudes** may also have an influence. Those participants who have a negative attitude towards any type of privacy violation are, in general, more motivated to complain. Those who are more difficult to motivate are those that:

– use the 'nothing to hide' argument: "*I don't talk about important things I need to be concerned about*", "*There is nothing I have to hide*",
– have become accustomed to privacy risks: "*nowadays it is normal*" , "*You don't have to like it, but in a way it has been wildly implemented for some years now, hasn't it?*", "*It's the same problem with computers. If anybody wants to be a criminal, there will always be a way*", "*On the internet via computer or smartphone data is saved as well*"
– think it is unavoidable : "*You can't change it*",

In summary, the following factors influence consumer ratings: the party who gathers the data; the type of data; awareness of the fact that (usage) data is collected; being aware that collected data can be misused; personalized advertising being considered beneficial, or not; basic attitudes.

5 Awareness-Raising Messages

In some pre-studies we tested a range of messages covering a combination of different influential factors (see Section 4.4). Some included concrete consequences other were more high level; some referred to hackers, others to vendors and broadcasters. We concluded that privacy-related awareness could best be prompted by messages that avoid being too specific about a potential misuse as too specific (e.g. burglary) is likely to be judged as low risk as it is considered as too unlikely in this context. People need to be able to visualize the particular scenario and believe that it could happen, i.e. it is realistic. Based on these pre-considerations, we decided to evaluate the following messages:

– **Simple awareness message.** : The Smart TV vendor and the broadcasters collect and analyze usage data (e.g., information about how, and how often, you use your Smart TV).
– **Advanced awareness message.** In addition to the text from the 'Simple awareness' Group: *It cannot be ruled out that the gathered information ends up in the wrong hands in order to harm you.*

Next, we wanted to evaluate how effective these messages would be and test whether the advanced message is more effective in terms of motivating participants to protect their privacy.

6 Methodology — Raising Awareness

In this section, we explain the study's design and the recruitment process. The ethical considerations and methodology were as described in Sections 3.3 and 3.4.

6.1 Study Design

The study applied a between-subjects design. Participants were randomly assigned to two groups that differed with respect to delivery of the above-mentioned awareness messages. The first group saw the simple message and the second group saw the advanced message. The study was proceeded through the following steps (see Figure 2):

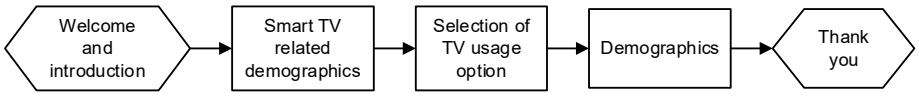

Fig. 2. Study Design.

Welcome and introduction: Participants were informed that the study focused on Smart TVs. They were not briefed about the exact focus so as not to prime their responses. Information about duration was provided (up to 10 minutes) as well as the fact that there were no wrong answers. They were told that they could leave the study at any point. However, only those who completed the study earned a monetary reward.
Smart TV related demographics: Participants were shown information related to Smart TVs and asked whether they owned a Smart TV. Afterwards, we presented information about Internet functionality and gave them some examples to illsutrate this. We then asked them to rate whether they use or would like to use Internet-related functionality on their Smart TV on a regular basis. Options ranged from 1 'does not apply at all' to 5 'fully applies'.
Selection of TV usage option: Participants were shown one of the two abovementioned awareness messages followed by an appropriate explanation of the message. Note that we did not call them simple or advanced. Participants were asked which Smart TV usage option they would prefer. Because the only truly reliable privacy protection option is not to connect the Smart TV to the Internet the following two usage options were presented[7]:

1. 'Privacy risk' option: The Smart TV will be connected to the Internet.
2. 'Privacy protecting' option: The Smart TV will not be connected to the Internet.

The **Demographics** and **Thank you** steps were as described in Section 3.1.

[7] the category names (privacy risk/protection) are only used here and were not communicated to the participants.

6.2 Recruitment

The studies were conducted in June/July 2016. SoSci Survey and clickworker were also used. We paid each participant who completed the studies and who did not provide obvious nonsense answers according to the minimum wage of Germany a fair monetary reward (i.e. €1.40 for about 9 minutes). Furthermore, we made sure that each clickworker could only fill out one of our Smart TV related studies.

7 Results — Raising Awareness

We report on the sample as well as the effectiveness of the awareness messages and the justifications.

7.1 Sample

155 participants completed the study. The study group consisted of 75 females (49%) and 79 males (51%); 1 participant did not mention gender.

We only considered those participants who stated that they own a Smart TV and who rated that they use Internet functionality regularly at least with 3 (ranged from 1 'does not apply at all' to 5 'fully applies').

82 (53%) participants owned a Smart TV and used Internet functionality regularly. From these 82, 43 (52 %) were made aware that usage data is collected and analyzed, i.e. were assigned to the 'simple awareness' group. The remaining 39 (48%) were assigned to the 'advanced awareness' group and were made aware that, in addition to legitimate collection and analysis, the data could also be misused to cause harm if accessed by criminals. The youngest participant in the 'simple awareness' group was 18, the oldest 65 and the mean age was 32.63 years with a standard deviation of 10.21. The corresponding numbers for the 'advanced awareness' group are: the youngest 18, the oldest 57, mean age 35.05 and standard deviation 11.20.

7.2 Effectiveness of Awareness Messages

In the 'simple awareness' group, 8 (19%) stated that they would not connect their Smart TV to the Internet anymore ('privacy protecting' option).

In the group 'advanced awareness', 15 (38%) participants selected this option. For more details see Table 2.

We did the following χ^2-tests: A significant improvement in the selection behavior could be shown between the groups 'Simple awareness' and 'Advanced awareness'; χ^2=4.00, df=1, p=0.046, ϕ-coefficient=0.221. Note, no significant difference could be found between males and females; 'Simple awareness': χ^2=4.51, df=1, p(exact)=0.06 and 'Advanced awareness': χ^2=0.37, df=1, p(exact)=0.74.

Table 2. Effectiveness of both awareness messages

	Simple awareness group			**Advanced awareness group**		
Option	**female**	**male**	$\sum$	**female**	**male**	$\sum$
# (%) Privacy risk option	17 (71%)	18 (95%)	35 (81%)	12 (57%)	12 (67%)	24 (62%)
# (%) Privacy protecting option	7 (29%)	1 (5%)	8 (19%)	9 (43%)	6 (33%)	15 (38%)
$\sum$	24	19	43	21	18	39

7.3 Justifications

The following categories of justifications for keep using the Internet were identified:

Functionality is important: Participants valued the functionality they obtained by connecting the Smart TV to the Internet. Example quotes are:

"A Smart TV without Internet isn't useful" , "I don't need a Smart TV without Internet", ,"If I own a Smart TV , I want to use [the Internet] functions", "I love the Internet", "The Internet extends the functionality of Smart TVs",

Some participants balanced privacy against functionality and functionality prevailed. Example quotes are:

"I think that the advantages that I get when it's connected to the Internet outweigh the disadvantages", "It is convenient to access the Internet on my Smart TV, but there is a risk that personal data will be stored"

Don't mind: Participants did not mind if usage data is collected and analyzed by broadcasters and vendors for various reasons. Example quotes are:

"I don't have any secrets in the selection of my programs", "I don't mind if my usage data is passed on" , "[..] I don't care if someone finds out that I watch porn."

Resignation: Participants were resigned to this use of their personal data. Example quotes are:

"I think nothing is wrong", "Today, data is collected everywhere. The recording of TV usage behavior is relatively innocent.", "Since data is stored in the Internet anyway. Moreover, it's a advantage because the offers are getting more personalized." , "The risk always exists that data ends up in the wrong hand, [..]." "There isn't 100% protection" ,"The risk always exist that data ends up in the wrong hand, [..]."

7.4 Discussion

This study's results demonstrate that significantly more consumers would disconnect their Smart TV when they are made aware of the risks with the advanced awareness message (with harm) as compared to the simple message (without

harm). Thus, for further awareness studies it is essential to communicate the potential harm and not just the fact that data is collected and analyzed.

We also gained other insights into Smart TV consumer attitudes towards privacy risks. Many would willingly sacrifice privacy in order to make use of the Internet functionality of Smart TVs either because (1) functionality is more important, (2) consumers do not mind sharing usage data or (3) consumers are resigned to privacy invasions. Note, most participants inhabited the first category.

Consequently, we were interested in whether the situation would change if privacy tools were made available. We wanted to evaluate the effectiveness of both messages in the presence of such a tool. In particular, we wanted to find out whether the advanced message was still more effective in this context.

8 Methodology & Results — Offering Functionality

The recruitment was carried out as described in Section 6.2. The ethical considerations and methodology were as described in Sections 3.3 and 3.4.

8.1 Study Design

The design was similar to the first study. Participants were given options as introduced in Section 6.1 and also an additional three other options[8]:

3. 'Effort' option: The Smart TV will not be connected to the Internet. It will be used as an external monitor for a laptop that is connected to the Internet.
4. 'Effort+cost' option: A privacy-protection mechanism will be deployed to prevent usage data collection while retaining Internet-enabled functionality. It will cost €20 and requires about 15 min to configure.
5. 'Costs' option: A privacy-protection mechanism will be deployed to prevent the usage data collection while retaining Internet-enabled functionality. It will cost €40 and no additional configuration time is required.

The privacy protection mechanisms with costs/effort have not been marketed as yet, but a prototype mechanism can be found in [19]. The 'Effort+cost' option is supposed to be installed on an existing device (e.g., router) and the software should be purchased for €20 similar to regular protection software for PCs[9]. The 15 minute configuration time is the average time a consumer may need to configure software (install it, choosing the preferences and select the right Smart TV Model). For the 'Costs' option, we considered a pre-configured bundle[10] with hard- and software which should be purchased for €40.

[8] We did not mention the names of the options in the study as presented here.
[9] See e.g. `https://www.amazon.com/dp/B010P91LYY` (accessed 11 December, 2016).
[10] See e.g. `https://www.amazon.com/dp/B000BTL0OA` (accessed 11 December, 2016).

8.2 Sample

169 participants completed the study. The study group consisted of 84 females (50%) and 83 males (50%); 2 did not provide gender. 97 (53%) participants owned a Smart TV and regularly used Internet-enabled functionality. From these 97, 45 (46 %) were assigned to the 'simple awareness' group and the remaining 52 (54%) were assigned to the 'advanced awareness' group . The youngest participant in the 'simple awareness' group was 18, the oldest 68 and the mean age was 36.44 years with a standard deviation of 12.08. The corresponding numbers for the 'advanced awareness' group are: the youngest 18, the oldest 67, mean age 36.80 and standard deviation 12.20.

8.3 Effectiveness of Privacy Protection Availability

Table 3 reports the results for all participants. In both groups more than 67% stated that they would be willing to spend time and/or money to get both functionality and privacy. From the three available options, the effort and/or cost options were preferred, especially in the 'advanced awareness' group (75%).

Table 3. Effectiveness of Both Messages

	Simple awareness group			**Advanced awareness group**		
Option	**female**	**male**	$\sum$	**female**	**male**	$\sum$
# (%) Privacy risk option	6 (27%)	8 (35%)	14 (31%)	4 (15%)	8 (31%)	12 (23%)
# (%) w/o Internet option	1 (5%)	0 (0%)	1 (2%)	1 (4%)	0 (0%)	1 (2%)
# (%) Effort option	3 (14%)	3 (13%)	6 (13%)	2 (8%)	4 (15%)	6 (12%)
# (%) Effort + costs option	7 (32%)	6 (26%)	13 (29%)	13 (50%)	12 (46%)	25 (48%)
# (%) Costs option	5 (23%)	6 (26%)	11 (24%)	6 (23%)	2 (8%)	8 (15%)
# (%) Costs and effort related options $\sum$	15 (68%)	15 (65%)	30 (67%)	21 (81%)	18 (69%)	39 (75%)
# (%) Privacy protecting options $\sum$	16 (73%)	15 (65%)	31 (69%)	22 (85%)	18 (69%)	40 (77%)
$\sum$	22	23	45	26	26	52

We applied the same χ^2-tests as in the first study. No significant improvement could be shown between the selection behavior of the 'simple awareness' and 'advanced awareness' groups; χ^2=4.21, df=4; p(exact)= 0.373.
There were no significant differences between male and female selections; 'simple awareness': χ^2=1.53, df=4, p(exact)=0.96 and 'advanced awareness': χ^2=4.83, df=4, p(exact)=0.28.

8.4 Effectiveness of Offering Functionality

We observed a difference in the choosing behavior of Smart TV consumers comparing the first (two options) and the second study (five options). We analyzed the differences between them. We found that an increased number of consumers demonstrated a preference for a privacy-protecting connection method.

For this analysis, we combined the groups 'w/o Internet' and all effort and/or cost groups from the second study to arrive at two groups. The distribution after combining the four privacy-protecting options of the second study looks, at first glance, like a random distribution, since 26 (27%) participants selected the 'Privacy risk' option and 71 (73%) a privacy-protecting option. A 20 to 80 distribution would be expected under random choice circumstances. In the first study, 59 (72%) wanted to retain the connection to the Internet and 23 (28 %) wanted to disconnect the Smart TV. Thus, the choice behavior differed significantly from a random distribution (χ^2=15.80, df=1, p¡0.001) with a clear lean towards the 'Privacy risk' option.

Therefore, we interpret the choice behavior in the second study as a positive effect. Proposing alternative options that protect the consumer's privacy while retaining Internet functionality seems the most promising approach.

9 Related Work

We report on related work in the following different areas:

Mental Models of Privacy and Security. Mental models can influence people's attitude, so we list some work in this field. Mental models in the context of privacy and security have been studied from Camp [2], Dourish *et al.*[10] and Wash [42] as well as in different concrete areas, such as smartphones from Ophoff *et al.*[29], Volkamer *et al.*[41], Harbach *et al.* [22] and Elie [11], network security from Solove[36], firewalls from Raja *et al.* [31], secure communication from Friedman *et al.* [12], passwords from Weirich *et al.* [44], single sign on Gupta *et al.* [20], anonymous credentials from Wäslund *et al.* [43] and Harbach *et al.* [21], privacy settings from Debatin *et al.* [6], email encryption from Gaw *et al.* [13], Renaud *et al.* [32] and Clark *et al.* [4]. In these areas, security and privacy protection tools are increasingly available. The focus of these papers differs from this work, since mental models should help us to understand why the existing tools are not used. We explored how consumers thought about Smart TV security and privacy risks in order to establish effective and acceptable protection measures. However, there are parallels. Some reasons for not using security tools might be reasons that consumers do not complain if corresponding tools are not available or vendors and broadcasters collect usage data intentionally.

Attitudes towards Privacy and Security. People's privacy attitudes often differ from the decisions they make. This inconsistency is called 'privacy paradox' . This issue has mostly been highlighted in the context of online privacy,

e.g., from Trepte *at al.* and Dienlein [39,7,38,40]. In the context of Smart TVs, we experienced similar issues. Consumers claimed that privacy was important, but most of them also connected their Smart TVs to the Internet without any qualms.

Privacy Calculus. The privacy calculus theory is one way to explain users' privacy behaviour (referred to as privacy paradox). It states that people seek a balance between potential risks and benefits, e.g. in e-commerce from Dinev *et al.* [8], in online market places from Kim *et al.* [23] or from Lankton *et al.* in social networks [25,3]. We discovered that, in the context of Smart TVs, functionality outweighs privacy concerns.

10 Discussion & Conclusion

We reported on three studies with a total 524 participants. They evaluated Smart TV owner awareness, attitudes towards privacy risks and measures to preserve privacy.

We had anticipated general lack of awareness. Our studies confirmed this. Only 28 of the 171 (16%) participants in the first study mentioned a privacy risks in their responses and only 12 (7%) were able to name concrete consequences of privacy invasions.

We showed that Smart TV consumers were most likely to deploy a privacy protection measure on their Smart TV when the measure did not impair available functionality. They were willing to commit time and/or effort to protect their privacy under these conditions. If functionality is restricted, on the other hand, they are unlikely to deploy a privacy-protection measure. Thus, corresponding usable technologies should be offered instead of purely making people aware of the privacy implications of current technologies.

Furthermore, we find that significantly greater numbers of Smart TV owners would disconnect their Smart TV when exposed to an awareness message that mentions actual potential harm. Thus, awareness-raising endeavours should always incorporate mention potential harms of Smart TV related privacy risks.
Further findings were:

- Some of our participants had become so used to being profiled and observed that they seemed to consider resistance futile.
- Others could only come up with the advantages of external agents collecting their data.
- Others demonstrated a naïve trust in vendors and broadcasters.

Limitations. All studies were conducted in Germany, where the population tends to be more attuned to privacy concerns than citizens of other countries [24]. A study with Americans, for example, might well deliver different awareness levels and responses to privacy risks. The studies relied on self-report. Participants could have given false answers but since they were anonymous it is hard to see that many would feel the need to disseminate or to fabricate responses. We

tailored surveys to reflect Smart TV privacy risks. A different set of scenarios might well have revealed other factors and thus led to dissimilar messages.

Acknowledgments

This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No 653454. It has also been supported by the German Federal Ministry of Education and Research (BMBF) within the project MoPPa (16KIS0343) and by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts within CRISP.

References

1. Working Group Smart TV of the German TV-Platform: Marktanalyse Smart-TV - Eine Bestandsaufnahme der Deutschen TV-Plattform , Last accessed on 06 November 2016, http://tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2013.pdf
2. Camp, L.J.: Mental models of privacy and security. Technology and Society Magazine, IEEE 28(3), 37–46 (2006)
3. Choi, B.C., Land, L.: The effects of general privacy concerns and transactional privacy concerns on facebook apps usage. Inf. Manage. 53(7), 868–877 (Nov 2016), https://doi.org/10.1016/j.im.2016.02.003
4. Clark, S., Goodspeed, T., Metzger, P., Wasserman, Z., Xu, K., Blaze, M.: Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System. In: USENIX Security Symposium (2011)
5. David Lodge: Is Your Samsung TV Listening To You?, Pen Test Partners. Accessed 23 February, 2016. Available from https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/
6. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication 15(1), 83–108 (2009)
7. Dienlin, T., Trepte, S.: Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology 45(3), 285–297 (2015)
8. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Info. Sys. Research 17(1), 61–80 (Mar 2006), http://dx.doi.org/10.1287/isre.1060.0080
9. DoctorBeet's Blog: LG Disables Smart TV features in the EU to force users to accept new oppressive Privacy policy, Accessed 23 February, 2016. Available from http://doctorbeet.blogspot.de/
10. Dourish, P., Delgado De La Flor, J., Joseph, M.: Security as a practical problem: Some preliminary observations of everyday mental models. In: Proceedings of CHI 2003 Workshop on HCI and Security Systems. Fort Lauderdale, Florida (5-10 April 2003)
11. Elie Bursztein: Survey: Most people don't lock their Android phones - but should (2014), https://www.elie.net/blog/survey-most-people-dont-lock-their-android-phones-but-should

12. Friedman, B., Hurley, D., Howe, D.C., Felten, E., Nissenbaum, H.: Users' conceptions of web security: A comparative study. In: CHI'02 extended abstracts on Human factors in computing systems. pp. 746–747. ACM (2002)
13. Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In: SIGCHI Conference on Human Factors in Computing Systems. pp. 591–600. CHI '06 (2006)
14. Ghiglieri, M., Waidner, M.: HbbTV Security and Privacy: Issues and Challenges. IEEE Security Privacy 14(3), 61–67 (May 2016)
15. Ghiglieri, M.: I Know What You Watched Last Sunday – A New Survey Of Privacy In HbbTV. Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy (2014)
16. Ghiglieri, M.: I Know What You Watched Last Sunday – A New Survey Of Privacy In HbbTV. Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy (2014)
17. Ghiglieri, M.: Incorrect HTTPS Certificate Validation in Samsung Smart TVs. Technical report (2014)
18. Ghiglieri, M., Oswald, F., Tews, E.: HbbTV – I Know What You Are Watching. In: Informationssicherheit stärken – Vertrauen in die Zukunft schaffen. pp. 225–238. Bundesamt fr Sicherheit in der Informationstechnik (05 2013)
19. Ghiglieri, M., Tews, E.: A Privacy Protection System for HbbTV in Smart TVs. In: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC). pp. 648–653 (01 2014)
20. Gupta, S., Bostrom, R.P.: Theoretical model for investigating the impact of knowledge portals on different levels of knowledge processing. International Journal of knowledge and Learning 1(4), 287–304 (2005)
21. Harbach, M., Fahl, S., Rieger, M., Smith, M.: On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In: Privacy Enhancing Technologies, pp. 245–264. Berlin Heidelberg. Springer (2013)
22. Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., Smith, M.: It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In: Symposium on Usable Privacy and Security (SOUPS). pp. 213–230 (2014)
23. Kim, G., Koo, H.: The causal relationship between risk and trust in the online marketplace. Comput. Hum. Behav. 55(PB), 1020–1029 (Feb 2016), http://dx.doi.org/10.1016/j.chb.2015.11.005
24. Krasnova, H., Veltri, N.F.: Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In: System sciences (HICSS), 2010 43rd Hawaii international conference on. pp. 1–10. IEEE (2010)
25. Lankton, N.K., McKnight, D.H.: What does it mean to trust facebook?: Examining technology and interpersonal trust beliefs. SIGMIS Database 42(2), 32–54 (May 2011), http://doi.acm.org/10.1145/1989098.1989101
26. Matyszczyk, C.: Samsung's warning: Our Smart TVs record your living room chatter (2015), http://www.cnet.com/uk/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/
27. Michéle, B., Karpow, A.: Watch and be Watched: Compromising All Smart TV Generations. In: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC). pp. 351–356 (01 2014)
28. Niemietz, M., Somorovsky, J., Mainka, C., Schwenk, J.: Not so Smart: On Smart TV Apps (undated), http://www.ei.ruhr-uni-bochum.de/media/nds/veroeffentlichungen/2015/08/31/SmartTvAttacks.pdf

29. Ophoff, J., Robinson, M.: Exploring end-user smartphone security awareness within a South African context. In: Information Security for South Africa (ISSA), 2014. pp. 1–7. IEEE (2014)
30. Oren, Y., Keromytis, A.D.: From the ether to the ethernet-attacking the internet using broadcast digital television. In: 23rd USENIX Security Symposium (USENIX Security 14). pp. 353–368 (2014)
31. Raja, F., Hawkey, K., Hsu, S., Wang, K.L., Beznosov, K.: Promoting a physical security mental model for personal firewall warnings. In: CHI '11 Extended Abstracts on Human Factors in Computing Systems. pp. 1585–1590. CHI EA '11, ACM, New York, NY, USA (2011)
32. Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why doesn't Jane protect her privacy? In: 14th International Symposium on Privacy Enhancing Technologies. Springer LNCS. pp. 244–262 (2014)
33. Rob Waugh (Metro): Smart TV hackers are filming people having sex on their sofas and putting it on porn sites, Last accessed on 06 November 2016, http://metro.co.uk/2016/05/23/smart-tv-hackers-are-filming-people-having-sex-on-their-sofas-and-putting-it-on-porn-sites-5899248/
34. Samsung: Samsung Privacy Policy–SmartTV Supplement, Last accessed on 06 November 2016, http://www.samsung.com/sg/info/privacy/smarttv/
35. Seven One Media: Addressable TV - The Future is now. (02), accessed 4 February, 2016. Available from authors on request
36. Solove, D.J.: "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. San Diego law review 44, 745 (2007)
37. Sony: Privacy Policy for the applications and/or online services on Sony's cloud platform, Accessed 23 February, 2016. Available from http://policies.sony.net/tvsideview/pp_en.htm
38. Trepte, S., Dienlin, T., Reinecke, L.: Risky behaviors: How online experiences influence privacy behaviors. Von der Gutenberg-Galaxis zur Google-Galaxis [From the Gutenberg galaxy to the Google galaxy] pp. 225–244 (2014)
39. Trepte, S., Reinecke, L.: Privacy online: Perspectives on privacy and self-disclosure in the social web (2011)
40. Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F.: Do people know about privacy and data protection strategies? towards the online privacy literacy scale(oplis). In: Reforming European data protection law, pp. 333–365. Springer Netherlands (2015)
41. Volkamer, M., Renaud, K., Kulyk, O., Emeröz, S.: A socio-technical investigation into smartphone security. In: Security and Trust Management, pp. 265–273. Springer (2015)
42. Wash, R.: Folk models of home computer security. In: Proceedings of the Sixth Symposium on Usable Privacy and Security. p. 11. ACM, Redmond, WA (2010)
43. Wästlund, E., Angulo, J., Fischer-Hbner, S.: Evoking comprehensive mental models of anonymous credentials. In: Camenisch, J., Kesdogan, D. (eds.) iNetSeC. Lecture Notes in Computer Science, vol. 7039, pp. 1–14. Springer (2011)
44. Weirich, D., Sasse, M.A.: Pretty good persuasion: a first step towards effective password security in the real world. In: Proc. of 2001 Workshop on New Security Paradigms. pp. 137–143. NSPW '01, Cloudcroft, NM (2001)
45. Zolfagharifard, E.: Is YOUR TV spying on you? Report reveals how Vizio smart televisions track your data so that it can be sold to advertisers (2015), http://www.dailymail.co.uk/sciencetech/article-3312597/Is-TV-spying-Report-reveals-Vizio-smart-televisions-track-data-sold-advertisers.html