Webcam Covering as Planned Behavior

Dominique Machuletz
University of Münster
Münster, Germany
D.Machuletz@uni-muenster.de

Stefan Laube
University of Münster
Münster, Germany
Stefan.Laube@uni-muenster.de

Rainer Böhme
University of Innsbruck
Innsbruck, Austria
Rainer.Boehme@uibk.ac.at

ABSTRACT

Most of today's laptops come with an integrated webcam placed beside the screen to enable video conferencing. Due to the risk of webcam spying attacks, some laptop users seem to be concerned about their privacy and seek protection by covering the webcam. This paper is the first to investigate personal characteristics and beliefs of users with and without webcam covers by applying the Theory of Planned Behavior. We record the privacy behavior of 180 users, develop a path model, and analyze it by applying Partial Least Squares. The analysis indicates that privacy concerns do not significantly influence users' decision to use a webcam cover. Rather, this behavior is influenced by users' attitudes, social environment, and perceived control over protecting privacy. Developers should take this as a lesson to design privacy enhancing technologies which are intuitive, usable and easy to understand.

ACM Classification Keywords

K.4.1. Computers and Society: Public Policy Issues—*Privacy*; H.5.m. Information Interfaces and Presentation (e. g. HCI): Miscellaneous

Author Keywords

Webcam cover; privacy; usability; Theory of Planned Behavior (TPB); Partial Least Squares (PLS); field study.

INTRODUCTION

The use of modern information technology (IT) comes with diverse privacy implications. Today's mobile devices are equipped with various powerful sensors and can store and forward large amounts of data at low cost. Several studies investigate data privacy risks regarding sensors, such as accelerometers [44], or biometric sensors [16]. Data privacy is defined as an individual's ability to decide which personal data is accessible to third parties [50]. If computing devices collect personal data and forward it without explicit consent, users' data privacy is violated. Sensor data is especially sensitive to privacy violations, as they may reveal highly intimate information about users' personal lives.

CHI 2018, April 21–26, 2018, Montreal, QC, Canada

ISBN 978-1-4503-5620-6/18/04…$15.00

DOI: https://doi.org/10.1145/3173574.3173754

A particular threat related to sensor data is the unauthorized video capture through webcams. If attackers can control webcams remotely, they may exploit highly sensitive video footage, which can cause serious harm to users. Some reported attacks on webcams were performed by *private attackers*, who threatened users to publish footage unless they pay a ransom (e. g., [18]). Beyond private attackers, *firms* might be interested in spying on their own employees through webcams [17]. Also, it is conceivable that *governments* spy on their citizens [47]. All such attacks are usually performed through Remote Administration Tools (RATs) that provide unobtrusive access to computing devices largely for malicious purposes [11]. Famous examples for RATs are *Blackshades* [20] and *Dark-Comet* [19]. For instance, such software was used by an attacker who spied on the Miss Teen of the USA and other women, threatening them to publish the footage [18]. Although the overall risk of spying attacks is deemed relatively small, many users seem to be concerned about being victims of such attacks [45, 42].

There are several ways to protect from webcam spying. On the software level, users can download tools that regularly check for spyware. On the Operating System (OS) level, they may uninstall drivers for the built-in webcam. On the Basic Input Output System (BIOS) level, it is in some cases possible to deactivate the functionality of the webcam altogether [22]. Yet, all of these measures require at least some computer literacy and thus cannot be adopted by inexperienced users. Besides, such measures are fairly inconvenient for users who, e. g., regularly participate in video conferences. To circumvent these issues, users may adjust the hardware of the computing device by sticking a piece of tape on the webcam lens, or by attaching a commercial webcam cover[1]. While certainly a pretty basic form of human-machine interaction, the use of webcam covers is intuitive to users, as its effectiveness is verifiable without requiring special skills or knowledge. Moreover, the use of webcam covers is observable, which enables us to study actual privacy behavior instead of relying on noisy measurements of self-reported behavior or behavioral intentions. The findings of our subsequent study may inform future research on privacy behavior as well as the design of usable privacy protection mechanisms.

Following up on the work by [37], our study systematically analyzes factors that lead laptop users to cover their webcam. We intend to overcome the two major deficiencies of the prior work, namely: (1) poor framing of questions, which

[1]There are several patents for commercial webcam covers, e. g., [23], [15], [27], [31], [8].

resulted in weak reliability scores and model fits, and (2) the missing evaluation of users' concern and perception regarding spying attacks on webcams, which lead to incomplete results regarding users' incentives for adopting webcam covering behavior. By overcoming these shortcomings, we intend to examine the reasons for users' decisions to cover their webcam or not. Our specific research question is:

Which factors influence users to protect their privacy by covering their laptop webcam?

In order to answer this question, it is suggestive to build on established theory which is proven to explain similar types of behaviors. We chose to apply the Theory of Planned Behavior (TPB). Developed by Fishbein and Ajzen [21, 3], TPB has become a cornerstone of many works in the behavioral sciences. The theory postulates that individuals' behavior is mainly influenced by their attitudes towards it, as well as their subjective norms and perceived behavioral control of performing this behavior. In the domain of data privacy, there exist studies that investigate these factors in isolation (e. g., [48],[6],[12]), while others specifically demonstrate that TPB can explain users' privacy protection behavior (e. g., [36], [32]). Thus, we suggest that this theory is also suitable for analyzing users' decision to cover their webcam. The TPB's constructs allow us to develop a latent factor path model which we can statistically verify. Required data was collected in the course of a field study, where we recorded laptop users' attitudes by standardized questionnaires while checking their laptops for a webcam cover. To the best of our knowledge, our study is the first to present robust results about the relationship between users' personal characteristics and their privacy behavior.

LITERATURE REVIEW

We summarize the existing research on users' perceptions regarding webcam spying attacks before we review studies on factors influencing users' general online privacy behaviors to motivate our theoretical and measurement approach.

Awareness and Concerns of Webcam Privacy Risks

Rouse [45] investigates how awareness and concerns regarding webcam spying attacks vary among different types of laptop users. Of 250 interviewed users, some are unaware (49%) that unauthorized parties may be able to access their webcams, while others (51%) express awareness when explicitly asked. Most of the aware users express concern over the possibility that their webcam may be hacked (79%). The author tests whether unaware users would get concerned if they become aware of possible attacks on webcams. Indeed, the briefing of formally unaware users lead most of them to become concerned (84%). The author concludes that, based on the high proportion of initially unaware participants, many users do not properly protect themselves against possible attacks on their webcam. He provides clear recommendations: users should stay informed about the risk, use antivirus software, close the laptop when it is not used, stick a cover on their webcam, and keep an eye on the laptop's activity indicator light.

A study by Portnoff et al. [42] specifically examines the effectiveness of webcam indicator lights in informing users about activities of their webcam. Based in a laboratory experiment, they find that less than half of their sample notices when the indicator is activated while sitting in front of a computing device. Additional interviews reveal that 13% of the participants are unaware of the fact that their webcam can be remotely controlled. When participants are asked to express their concerns about possible spying attacks, many state that they would be afraid of intimate details being exposed to the public. Also, many participants claim that they would immediately cover their webcam if the indicator light turns on unexpectedly. The authors conclude that webcam indicator lights have limited effectiveness, highlighting the need for better designed privacy indicators which can enable users to self-protect when noticing a potential attack. The work by Mirzamohammadi and Sani [38] presents a solution for trustworthy sensor notifications. These authors address concerns about attacks on various sensors of mobile devices by implementing a system which provides users with immediate feedback when sensors, such as the microphone or camera, are being used by applications. To ensure that users actually notice the indicator, they not only use the devices' LED, but also the vibrating motor and display as warnings of potential attacks.

We are only aware of one paper [37] which specifically addresses webcam covering as a means to self-protect against webcam spying attacks. Using bivariate statistical methods, the authors find that laptop users who state that webcam covers are a useful and practical protective measure are significantly more likely to actually cover their webcam. This suggests that users' attitudes towards webcam covering has some impact, but the interaction with other factors remains elusive.

Overall, the reviewed studies conclude that users need better education about the potential risk of webcam spying. Yet, the studies do not precisely investigate if concerns about this risk cause users to actually adopt self-protection, or if other factors, such as those suggested by the TPB, explain protection behavior. Our study closes this gap by systematically investigating the relationship between users' webcam covering behavior and attitudes, subjective norms, and perceived behavioral control.

Factors Influencing Users' Privacy Behavior

The adoption of various privacy behaviors is often analyzed by using factors which are comprised in the TPB, but without explicit reference nor complete application of the theory. For instance, researchers examine the impact of users' *attitudes*. Several studies report a discrepancy between users' privacy attitudes and their corresponding online privacy behaviors. In the privacy literature, this discrepancy is often framed as a "privacy paradox" [39]. Spiekermann et al. [48] were among the first to point out this discrepancy. They compare Internet users' privacy attitudes and their privacy behavior when shopping online by assessing self-reported privacy preferences of 206 participants, while observing their disclosure behavior at a simulated online shop during a laboratory experiment. They find that most participants highly value their privacy, but do not behave accordingly, as many of them reveal personal data to the shop. Several other studies concur (e. g., [6], [39], [1]). The paradox may be explained by users' lack of awareness of potential risks [2], or by arguing that users do not adopt privacy measures because of poor usability [35].

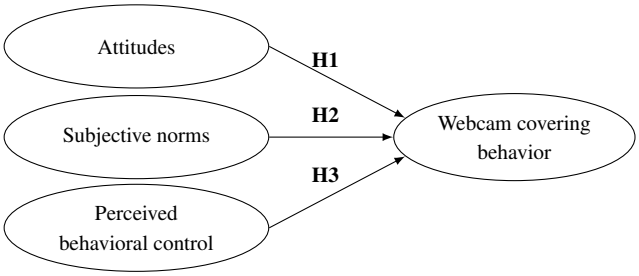

Figure 1. Research model

Besides attitudes, researchers investigate the effect of users' *social environment* on privacy behavior. For example, Lee and Kozar [34] examine factors influencing users' intentions to adopt anti-spyware systems by handing out questionnaires to 292 Internet users. They find that female users' decision to adopt anti-spyware systems is significantly influenced by other peoples' opinions, implicating that women are affected by pressure from their social environment. Contrarily, there is no significant effect for male participants in the study. Böhme and Pötzsch [9] study personal data disclosure decisions from the lens of descriptive, as opposed to injunctive, social norms. They report evidence for people adjusting their own privacy behavior to observable disclosures of relevant others by analyzing data collected from an online social lending platform. However, their method did not allow for inclusion of self-reported factors, such as awareness of and attitudes towards the risk. In contrast, Lwin and Williams [36] do not find that the social environment has any influence on privacy behavior. They conduct an online survey with 341 participants to investigate factors that lead online users to purposefully provide wrong personal data on websites. Among other aspects, the authors ask participants to state to which level their family members', friends' and other acquaintances' opinions are relevant when deciding to fabricate personal data online. The analysis does not indicate any statistically significant effect of other people's opinions on study participants' decision.

Moreover, researchers analyze how users' *perceived ability to control* their personal data impacts their actual privacy behavior. For example, Hughes-Roberts and Kani-Zabihi [32] test how online social network website interface (UI) designs influence users' information disclosure behavior. The authors do so by testing different UIs on 45 university students, and analyzing their disclosed data. They find that users who test UIs that lead them to perceive a high level of control over their personal data are less likely to disclose. Brandimarte et al. [10] report different results. They conduct three online experiments with a total of 398 Internet users. Participants are provided with varying levels of control over the website's information release of their personal data. The results indicate that users with higher control perception are significantly more likely to reveal sensitive data about themselves.

As many of the mentioned studies report that users' privacy behavior is significantly influenced by their attitudes, social environment, and control perceptions, we conjecture that webcam covering behavior is multi-causal. As all discussed factors appear as constructs in the TPB, we decided to build our work on this theory and adopt its rigorous measurement approach.

RESEARCH MODEL AND HYPOTHESES

Our TPB-based research model is depicted in Figure 1. The TPB posits a relationship between personal beliefs, behavioral intentions, and behavior. According to the TPB, behavior needs to be defined as (1) an observable action (2) towards a specific target (3) at a specified time (4) in a specific context [5, p. 2]. In our study, this action is the usage of a webcam cover, the target is the users' laptop, the point in time is the time of our research contact, and the context represents the public places visited during the field study. In the original theory, behavioral intention is the direct antecedent of behavior. Our research model skips this mediator, because intentions reflect behaviors which are performed in the future. As we collect data on users' webcam covering behavior and on their personal beliefs at the same time, measuring the intention of covering the webcam becomes redundant. Thus, we focus on personal beliefs, i. e., the predecessors of intention: attitudes, subjective norms, and perceived behavioral control. We expect a direct positive relationship between these factors and users' webcam covering behavior, and thus can formulate three hypotheses.

Our first hypotheses concerns users' attitudes towards webcam covers. Attitudes reflect the degree to which someone has a positive or negative evaluation on the behavior and its envisaged outcomes [4, p. 188]. We assume that users who mainly hold positive attitudes towards webcam covers, such as perceived usefulness, are more likely to cover their webcam. Accordingly, we assume that negative attitudes, such as the perception that a cover is distracting, cause users to abstain from webcam covering. Hence, our first hypothesis is:

H1 Users who report to hold positive attitudes towards webcam covers are more likely to cover their webcam than users who report to hold negative or neutral attitudes.

Our second hypothesis addresses the influence of users' subjective norms on covering behavior. Subjective norms signify users' overall perceptions regarding expectations and opinions of people in their social environment [4, p. 195]. We expect that such perceptions impact users' decision to adopt this privacy measure, since webcam covers on laptops are usually visible to the surrounding. Thus, our second hypothesis is:

H2 Users who report to perceive positive subjective norms towards webcam covers are more likely to cover their webcam than users who report to perceive negative or neutral subjective norms.

Our third hypothesis focuses on users' perceived behavioral control when using a webcam cover. Perceived behavioral control represents one's subjectively evaluated capability of performing a behavior, and thus achieving its envisaged outcome [4, p. 197]. An underlying premise of this study is that all users possess the required resources, and are in principle capable of covering their webcam by sticking a cover on the webcam lens of their laptop. Yet, we suggest that users who are of the opinion that covering the webcam leads to more control over protecting themselves from spying attacks by various attacker types are more likely to use a cover. Hence, our focus lies on users' control perception over the privacy protection mechanism of a cover. We formulate our third hypothesis as:

H3 Users who report to have a positive perceived behavioral control in protecting privacy through a webcam cover are more likely to cover their webcam than users who report to have a negative or neutral perceived behavioral control.

INSTRUMENT

To test our proposed hypotheses, we created a questionnaire and conducted a field study. Subsequently, we introduce our measurement approach for eliciting users' attitudes, subjective norms, and perceived behavioral control, as well as their actual behavior. Then, we present how we assess users' additional personal characteristics and describe how we pretested the questionnaire. Finally, we describe our survey procedure.

Measurement of TPB constructs

Following Ajzen's guidelines for constructing a TPB questionnaire [5], we conducted a small pre-study. By doing so, we were able to elicit the target group's commonly held beliefs about webcam covering while avoiding that only beliefs held by the researchers are included in the questionnaire of the main study. Specifically, we recruited 13 users who regularly use their laptop at public places, and asked them to fill out a short questionnaire including 7 open-ended questions regarding their opinions about webcam covers. These questions concern users' perceived advantages, disadvantages, social implications, further associations with webcam covering behavior, and their beliefs about potential attackers on webcams.

The results of the pre-study allowed us to create several items for measuring laptop users' attitudes, subjective norms, and perceived behavioral control regarding webcam covering, reported in Table 1.[2] All items are anchored on a seven-point rating scale ("Strongly disagree" to "Strongly agree"). While some items consist of a single survey question, others are weighed by a further question, assessing the degree to which a participant evaluates the addressed aspect. We apply these weightings to aspects which need to be measured by both expectation and evaluation (e. g., "It distracts me when my webcam is covered." is weighted by "It is important for me to use my laptop without any distractions."). This method is recommended by Ajzen [5, p. 9] who claims that it provides better insights about participants' considerations when deciding to perform or to not perform the behavior.

Items on attitudes refer to the overall evaluation of webcam covering behavior. We include items addressing laptop users' perceived advantages (ATT1, ATT2) and disadvantages (ATT3, ATT5) from using webcam covers, as well as their perception of being observed if their webcam is not covered (ATT4).

Items on subjective norms include social implications of using webcam covers, and opinions of important people within users' social environment. We ask to which degree laptop users feel uncomfortable when their webcam cover is exposed to their surrounding (SN1, SN2). Furthermore, participants had to rate their evaluation of other people's opinions regarding webcam covers (SN3). This item focuses on people whose opinions on online privacy are valued by the user.

[2]Note that items are translated from the originally German wordings.

Item	Item translation
Attitudes	
$ATT1_{W1}$	Webcam covering is a useful online privacy protection measure.
ATT2	When I cover my laptop webcam, I feel more at ease while using my laptop.
$ATT3_{W2} \leftrightarrow$	It distracts me when my webcam is covered.
ATT4	When my webcam is not covered, I have the feeling to be observed while using my laptop.
ATT5 $\leftrightarrow$	I feel that covering my webcam is an excessive privacy protection measure.
Subjective norms	
SN1 $\leftrightarrow$	Others might think that I am paranoid when my webcam is covered.
SN2 $\leftrightarrow$	It embarrasses me if my webcam is covered.
$SN3_{W3}$	People whose opinions regarding online privacy protection I value would endorse me to cover my webcam.
Perceived behavioral control	
$PBC1_{W4}$	I have more control over my online privacy if I cover my webcam.
$PBC2_{W5}$	Webcam covering protects me against spying attacks from foreign intelligence agencies.
$PBC3_{W5}$	Webcam covering protects me against spying attacks from domestic intelligence agencies.
$PBC4_{W5}$	Webcam covering protects me against spying attacks from criminals.
$PBC5_{W5}$	Webcam covering protects me against spying attacks from Internet firms.
$PBC6_{W5}$	Webcam covering protects me against spying attacks from people in my surrounding.
Weighting	
W1	It is important for me to protect my privacy when being online.
W2	It is important for me to use my laptop without any distractions.
W3	I do what people whose opinions regarding online privacy protection I value argue for.
W4	It is important for me to have control over my privacy when being online.
W5	I consider it necessary to cover the webcam.

Table 1. Translation of TPB items. Items marked with 'W' are weighed by the corresponding item from the last section of the table. Scales of items marked with '$\leftrightarrow$' were reversed for the PLS analysis.

Items measuring perceived behavioral control concern laptop users' perceived ability to protect their online privacy by means of a webcam cover. We ask participants to evaluate their overall control perception when using a cover (PBC1). Also, we include specific questions addressing possible attacker types (PBC2–PBC6). By asking laptop users to rate their ability to protect themselves from different attacks by using a cover, we are able to investigate beliefs about the type of potentially occurring attacks on their webcam.

The construct behavior is reflected by a single binary item indicating whether the subject uses a webcam cover or not. A single binary item is sufficient as there is little risk of measurement error when we directly observe a user's laptop.

Measurement of Further Personal Characteristics

In addition to items measuring the TPB constructs, the questionnaire includes further items that address laptop users' personal characteristics. A translation of these items is reported in Table 2 in the appendix. Specifically, we obtain participants' demographic information (I1–I8), usage behavior (I9–I14), and potential incentives for and against adopting webcam covering behavior, such as user concerns (I15–I20). This data enables us to conduct an extended analysis backing up our results from examining the proposed hypotheses.

Pretests

The resulting questionnaire consisting of the TPB items and the additional questions was tested and iteratively improved to minimize possible difficulties of comprehension which may limit the explanatory power of the obtained data. For this purpose, we followed Prüfer et al. [43] and conducted 11 semi-structured interviews with potential study participants. During these interviews, we applied the common pretesting techniques *thinking aloud*, *probing*, *confidence rating*, and *paraphrasing* to determine participants' understanding of items.

Survey Procedure

Data collection took place in December 2016 at various public places in and around a college town in the north-western part of Germany. Specifically, we chose places populated with people currently using their laptops, e. g., commuter trains and public libraries. All German-speaking laptop users in these places were considered as suitable candidates for our research. We approached these users and asked them to participate in a study on online privacy protection behavior, and offered them a chocolate bar as a compensation for their participation. The briefing mentioned the approximate duration of the procedure (10 to 15 minutes). After participants' agreement, we handed them the questionnaire to be filled out. Meanwhile, we unobtrusively noted down whether a webcam cover was attached to the laptop. After completing the questionnaire, we informed them about the observation. Moreover, we assured that all responses are held confidential and cannot be linked to their identity. Our total sample size is 180 laptop users.

In fulfillment of approved ethical standards, we only recorded observations of users who agreed to participate in our study. Thus, we are not able to provide exact numbers about the percentage of (non-)cover users who declined to participate. The interviewers guess that on average, three out of four approached laptop users did not agree to take part. It is possible that users protecting their privacy were more likely to participate as they might be more interested in the topic. Thus, webcam cover users could be overrepresented in our sample.

DATA ANALYSIS

We first discuss personal characteristics that do not directly fit into the TPB constructs and analyze their relation to webcam covering behavior. Then, we present the statistical model used to test our TPB-based research model and hypotheses.

Descriptive Analysis

This initial analysis characterizes our sample and offers a first idea of factors influencing webcam covering, albeit without rigorous theory and on the level of bivariate statistics only.

Item	Item translation
I1	What is your gender?
I2	In which age category do you belong?
I3	What is your highest level of education?
I4	Which occupation type are you currently in?
I5	If you are a student, what is your course of study?
I6	Have you ever programmed a computer program or a website?
I7	How would you rate your knowledge regarding information technology?
I8	How would you rate your knowledge regarding computer security?
I9	How much time per day do you on average use your laptop?
I10	How often do you use the webcam of your laptop?
I11	Is your laptop password-protected?
I12	Is there antivirus software installed on your laptop?
I13	Have you ever deleted the *cookies* of a browser on your laptop?
I14	Do you use a mobile phone privacy filter on your display to avoid lateral glances on your mobile phone?
I15	I am concerned that the webcam on my laptop could be controlled remotely by an unauthorized party.
I16	If the webcam on your laptop is currently covered, what induced you to do so?
I17	If the webcam on your laptop is currently not covered, had it been covered in the past?
I18	Do you think you would notice if an unauthorized party remotely controls the webcam on your laptop?
I19	Do you believe that an unauthorized party has remotely controlled the webcam on your laptop in the past?
I20	Do you know someone from your social environment who in the past experienced that an unauthorized party remotely controlled their laptop webcam?
I21	Do you own any other devices (e. g., tablets, smartphones or other laptops) with a covered webcam/camera?

Table 2. Translation of additional items

Demographics

Table 3 reports the survey demographics. Recall that corresponding item codes (I1–I21) are given in Table 2. In total, 36% of all laptop users in our study were observed with a covered webcam. Somewhat surprisingly, and reassuringly, this marginal distribution matches the proportion of webcam cover users observed in prior work [37] whose data collection took place more than a year earlier (also in Germany).

When analyzing the gender distribution (I1), we find noteworthy differences between male and female participants. A larger proportion of female participants uses a webcam cover (45%) in comparison to male participants (25%). Fisher's exact test confirms that the difference between those two groups is statistically significant ($p < 0.05$).

Regarding the age distribution of our sample (I2), it is notable that most of our participants (68%) are 25 years or younger. This can partially be explained by the general age distribution of laptop users in Germany [30]. When examining the use

of webcam covers by age groups in more detail, we observe some differences: while more than a third of all participants between age 21 and 25 use a cover, the ratio is only 20% in the age bracket from 31 to 40. Yet, we cannot find statistically significant relations between age and webcam covering.

When examining the participants' highest completed level of education (I3), we find that users of almost all educational backgrounds use webcam covers. Except for the two postdocs in our sample, at least a quarter of each remaining group uses this privacy measure. Covers are most prevalent in the group of participants with a secondary school degree (42%).

More than half of our participants are university students (57%), of which 38% cover their webcam (I4). It is notable that a higher proportion of university students who are enrolled in a non-technical study program (I5) cover their webcam (43%) in comparison to the group of technical students (28%). However, it has to be considered that significantly more men than women are enrolled in technical study programs (Fisher's exact test, $p < 0.001$). To test which of the two variables affects webcam covering behavior, we perform a logistic regression with the independent binary variables *gender* and *technical course of study*, and the dependent binary variable *webcam covering behavior*. The estimated coefficients reveal that only *gender* significantly influences *webcam covering behavior* (Estimate$= 1.07, p < 0.05$), while *technical course of study* does not have a visible impact (Estimate$= -0.20, p = 0.68$). Thus, the observation that more non-technical students cover their webcam can be explained with the gender distribution.

We also asked the participants to state whether they have programming experience (I6) and to self-assess their level of knowledge about IT (I7) and computer security (I8). We find that participants with and without programming experience are equally likely to use webcam covers. Furthermore, of all participants who state to have no knowledge about IT, a large proportion was observed with a webcam cover (46%). Only 25% of participants who claim to be experts in computer security cover their webcam. These findings show that webcam covering can be adopted by users who have very little knowledge about IT and computer security, underlining the simplicity and intuitive nature of this privacy measure.

Stated Usage Behavior

We asked the participants to answer several questions on their usage behavior. For example, we asked for the average time of laptop use per day (I9), and how often participants use their webcam (I10). Surprisingly, no statistically significant relation between webcam covering and these usage indicators can be found. In fact, even participants who report to use their webcam every day were observed with a cover. It seems to be very important for these users to protect their privacy by covering the webcam, as they make the effort of putting the cover off and on every time they, e. g., join a video conference.

Furthermore, we analyze if laptop users using other security/privacy measures are more likely to cover their webcam. To this end, we asked participants to report whether they protect their laptops by using passwords (I11), have antivirus software installed (I12), delete cookies of their browser (I13), and use a privacy filter on their mobile phone, protecting against lateral glances (I14). In summary, a higher percentage of participants who adopt these measures also use a webcam cover in comparison to those who do not. It is striking that a large share of all users making use of privacy filters additionally cover their webcam (75%). This result shows that users who employ other privacy protection measures, especially those which affect the physical appearance of computing devices, are likely to also use webcam covers.

Item (Item code)	Total	With cover	
All	180	65	36%
Gender (I1)			
Male	79	20	25%
Female	100	44	45%
Age (I2)			
<18	26	9	35%
18-20	34	14	41%
21-25	62	21	34%
26-30	26	7	27%
31-40	10	2	20%
41-50	9	6	67%
51-60	6	1	17%
>60	2	1	50%
Education (I3)			
No school-leaving qualification	19	5	26%
Secondary school	24	10	42%
High school	78	27	35%
Bachelor	41	15	38%
Master	9	3	33%
PhD	2	0	0%
Occupation type (I4)			
High school student	32	11	34%
University student	102	39	38%
Full-time employment	38	9	29%
Half-time employment	8	4	50%
Retired	2	0	0%
None	2	1	50%

Table 3. Demographics

We also find that 3.8% of all users in our sample report to cover the camera on their phone, while a total of 4.4% use a cover on their tablet (I21). One explanation for these rather small numbers may be that privacy behavior is less driven by concerns about potential spying attacks, but rather by perceived convenience. For instance, it is more convenient to remove a webcam cover before a video call than before taking a photo with one's phone.

Motivations for Webcam Covering

In order to learn more about laptop users' motivations to make use of webcam covers, we asked participants several questions regarding their concerns, incentives, and past experiences.

For assessing laptop users' overall fear of webcam spying, we asked the participants to rate the level of privacy concern on a 7-point scale (I15). The majority (58%) chose a value of 5 or higher. Of those who are highly concerned (value of 6 or 7), 57% make use of a cover. Of all unconcerned participants

(value of 3 or less), 10% use a cover. Surprisingly, of those participants stating to be not at all concerned (value of 1), still 16% cover their webcam. Overall, we do not find a significant correlation between concern and webcam covering. From these results we conclude that concern does not sufficiently explain why people make use of webcam covers.

We asked the participants with webcam covers in an open-ended question to describe why they have decided to use a cover (I16). Many of them responded briefly that they use a cover to protect their privacy (15%), or to protect themselves from spying attacks (17%). Others named specific persons from their social environment, e. g., family members, friends, or teachers, who motivated them to cover their webcam (14%). Some explained that media reports about webcam spying attacks, or about famous people who cover their webcam (e. g., Edward Snowden and Mark Zuckerberg), have inspired them (12%). The most frequently expressed reason was an uncomfortable feeling of being watched when being exposed to an uncovered webcam (29%). Only one participant stated that he covers his webcam because he believes to have experienced an actual spying attack in the past.

We also asked users without a webcam cover whether they had been using one in the past (I17). Of all participants without cover, 20% reported that they had been covering their webcam at an earlier point in time. Of these users, 29% named inconvenience as a reason for discontinuing to do so, while 12% pointed to the uncomely appearance of a webcam cover.

During our observation procedure, we also noted down the type and appearance of users' webcam covers. While the majority of all covers were stickers or paper and tape, 8% were commercial webcam covers that can be opened and closed manually. Moreover, we recorded whether covers are very obvious to the surrounding, e. g., because of bright colors, or whether they are rather discreet. We find that 48% of all webcam cover users made some effort to hide the cover by choosing stickers in the color of their device. We conjecture that the outer appearance of laptops is important to webcam cover users, or that these are to some extent embarrassed to reveal that they cover their webcam.

Furthermore, we asked participants to state whether they think that they would notice a webcam spying attack if it happened to them (I18). The vast majority of all participants claimed that they would not be able to recognize such a spying attack (86%). The ratio is even higher (91%) for users of webcam covers. This result relates to the findings of Portnoff et al. [42], who point out that the webcam indicator light goes unnoticed by many laptop users.

When asking about past experience with unauthorized webcam spying (I19), 11 participants (6%) claimed that they had been victims of such an attack, of which 7 (64%) use a webcam cover. Moreover, of all participants, 10 (6%) know a person in their social environment that claims to have experienced a webcam spying attack (I20). Of these participants, 6 (60%) were observed with a cover. From these results we can derive that the belief of having been victim of a spying attack, or knowing someone who claims to have experienced an attack, can explain why users take precautionary measures. However, even after accounting for possible response biases, the fraction of users with direct or indirect negative experience appears too small to fully explain an adoption rate of 36%. This calls for a multi-causal explanation of webcam covering behavior, which we do in the following on the basis of the TPB.

	Construct			
Item	*ATT*	*SN*	*PBC*	*BEHAV*
ATT1	**0.84**	0.47	0.74	0.49
ATT2	**0.91**	0.38	0.73	0.52
ATT3	**0.65**	0.49	0.44	0.42
ATT4	**0.83**	0.36	0.73	0.52
ATT5	**0.83**	0.51	0.63	0.51
SN1	0.40	**0.79**	0.33	0.34
SN2	0.36	**0.77**	0.28	0.31
SN3	0.43	**0.68**	0.45	0.40
PBC1	0.55	0.26	**0.61**	0.34
PBC2	0.72	0.42	**0.93**	0.57
PBC3	0.71	0.39	**0.91**	0.54
PBC4	0.80	0.50	**0.92**	0.57
PBC5	0.76	0.47	**0.92**	0.58
PBC6	0.55	0.39	**0.74**	0.39
B	0.61	0.48	0.60	**1.00**

Table 4. Cross loadings

Research Model Evaluation

We now proceed with testing the proposed TPB hypotheses. For our analysis, we employ the PLS method, which is often used in TPB studies (e. g., [41], [40], [25]). PLS fits path models that include both multiple regression and factor analyses while accommodating latent factors, i. e., constructs that are not directly measurable. Therefore, it is suitable for modeling the TPB constructs *attitudes* (*ATT*), *subjective norms* (*SN*) and *perceived behavioral control* (*PBC*), which are not measured directly, but are reflected by several items each. Also, the connection between these constructs and *behavior* (*BEHAV*) can be examined. The PLS analysis includes two stages: the measurement model and the structural model. The former links observed items to their respective constructs, while the latter reflects the connection between these constructs [13].

We conduct our analysis by using the R package `plspm` [46]. Of our initial 180 response records, we discard those with more than three missing values in the variables relevant for the PLS analysis. In total, the data set includes 8 records with missing values of which this rule applies to two. The missing values of the remaining 6 records are replaced by mean imputations. Consequently, the following analysis uses 178 cases.

Measurement Model

To assess the reflective measurement model, we test for indicator reliability, construct reliability, convergent validity, and discriminant reliability, as suggested in the methodological literature [14, 28, 26]. This is done to provide assurance that items measure the constructs they are intended to measure.

For establishing indicator reliability, we calculate the factor loading for each item (bold values in Table 4). Factor loadings

Construct	Items	CR	AVE
ATT	5	0.91	0.66
SN	3	0.79	0.56
PBC	6	0.94	0.72
BEHAV	1	1.00	1.00

Table 5. Composite reliability and average variance extracted

Construct	*ATT*	*SN*	*PBC*	*BEHAV*
ATT	**0.812**			
SN	0.538	**0.747**		
PBC	0.811	0.487	**0.846**	
BEHAV	0.608	0.477	0.602	**1.000**

Table 6. Fornell–Larcker criterion analysis

measure how well an item explains its respective construct. Hair et al. [28] state that factor loadings should at least be 0.7. Yet, it is acceptable to have a few items with less loading, since this is a common phenomenon for newly designed scales [14]. All of our 15 items have a factor loading on their respective construct higher than 0.61. 12 items exceed the value of 0.74. We deem this result acceptable as the scales in our study are newly developed and contain reversed items (without reversed items, response patterns may inflate the reliability).

Construct reliability indicates a construct's internal consistency, meaning that items belonging to the same construct generate similar values. According to Hair et al. [28], a reasonable metric is the composite reliability index (CR) ranging from 0 (absolutely unreliable) to 1 (absolutely reliable). Acceptable thresholds for this index lie above 0.6 for exploratory research, while values above 0.7 are recommended for more advanced research stages. Table 5 reports the CR values of our constructs. They are above 0.79, indicating strong internal consistency of our constructs despite the use of reversed items.

Convergent validity reflects the degree to which a construct's items are related. To assess convergent validity, we have to assure that the items share more variances with their respective construct than with the remaining constructs by examining the average variance extracted (AVE) (Table 5). In detail, the AVE of each construct should have a value of 0.5 or higher [33]. This indicates that more than 50% of the variances of each item are explained through its respective construct. All our constructs' AVE values are above 0.56, indicating acceptable convergent validity.

Discriminant validity, which indicates whether the constructs of the model differ from each other, is usually established using cross loadings (Table 4) and the Fornell–Larcker criterion (Table 6). Cross loadings reflect how each item loads on each construct of the model. To establish discriminant validity, each item must load highest on its respective construct. As evident from Table 4, all our items satisfy this requirement. The Fornell–Larcker criterion is met if the square root of the AVE value of each construct is higher than its highest correlation with the remaining constructs. Table 6 reports the square roots of each construct's AVE value (bold values on the diagonal) and the correlations between the constructs. As evident, all constructs fulfill the Fornell–Larcker criterion. Overall, the analysis of the measurement model suggests that the quality of the proposed items is acceptable. Therefore, our research model is suitable to be analyzed and interpreted in more detail.

Structural Model

For the evaluation of the structural model, the three relevant path coefficients between the constructs are determined through bootstrapping with a sample size of 500 [46] (Figure 2). Path coefficients reflect the constructs' relationship by indicating their direction and size [28]. All path coefficients of our model are positive and statistically significant, SN and PBC even on the 0.01 level. The overall explanatory power of the structural model is indicated by the coefficient of determination (R^2) of the endogenous construct behavior. Our model explains 44% of the variance of webcam covering behavior. This is substantially more than any of the individual causes alone. R^2 values are highly domain-specific and we are not aware of statistically justifiable thresholds. Chin [13], in search for a rule of thumb, calls values above 0.333 "moderate" [46]. Overall, we deem the explanatory power of our model good enough for further interpretation.

For additional verification of the predictive power of our model, we obtain Stone–Geisser's Q^2 [49, 24] by applying blindfolding procedures and skipping every fifth data point of the single binary indicator of the endogenous and reflective construct behavior. Then, the calculated estimates predict the skipped data points. Since our Q^2 value for cross-validated redundancy is 0.44, and thus greater than zero, the proposed model has non-negligible predictive power [29].

As we observe significant differences between male and female participants in terms of their propensity to cover the webcam, we are as well interested if males' and females' webcam covering behavior is differently influenced by their attitudes, subjective norms, and perceived behavioral control. To detect differences, we apply a bootstrap t-test. With this procedure, the response records are separated into two groups. Then, bootstrap samples are run for each group to calculate the path coefficients. The estimated standard errors are used in a parametric sense through a t-test. The results show that there are no significant differences between the path coefficients of the two groups (ATT: $t(176) = 0.69$, $p = 0.25$; SN: $t(176) = 0.14$, $p = 0.44$; PBC: $t(176) = 1.18$, $p = 0.12$). Thus, male and female users' determinants for their webcam covering behavior do not differ significantly.

Moreover, we test if laptop users' overall level of concern regarding spying attacks additionally influences their decision to cover the webcam. We do so by inserting a control variable into our TPB-based model. This control variable is reflected by a single item measuring users' concern on a 7-point rating scale (I17). The analysis of this model reveals that after controlling for the TPB factors, there is no significant impact of concern on webcam covering behavior ($p = 0.74$). In other words, the TPB items contain all relevant information to explain the phenomenon (to the extent possible in this study).

DISCUSSION

We are now able to discuss the postulated hypotheses and answer our research question. Thereafter, we propose theoretical implications for future research, as well as practical implica-

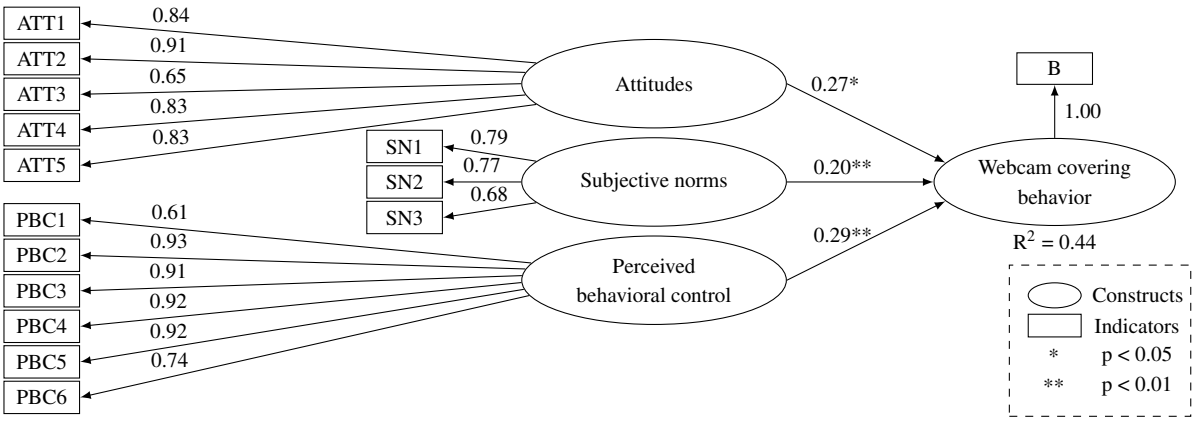

Figure 2. PLS path coefficients

tions targeted at designers of privacy enhancing technologies. Finally, we discuss the limitations of this study.

Revisiting the Hypotheses

Supporting H1, we find that attitudes regarding webcam covers significantly impacts users' decision to attach a cover on their webcam. The item loading highest on this construct measures that participants feel at ease when using a webcam cover (ATT2). This indicates that a covered webcam promotes a comfortable feeling for many laptop users. The result also corresponds to the most frequently given answer when asking open-ended for the reason to deploy a webcam cover (I16): most laptop users with a cover stated that they feel uncomfortable when exposed to an uncovered webcam. In line with this, the high loading of item ATT4 underlines that the feeling of being watched when the webcam is uncovered leads users to adopt webcam covering behavior. Users who are distracted by a cover (ATT3) and think of it as an excessive privacy measure (ATT5) are less likely to use one. Thus, perceived usability limitations significantly influence users' decision to cover their webcam. This goes in line with our finding that 20% of all users without cover stated that they had used a cover in the past, but now abstain from it mainly because they did not perceive it as usable. Overall, the significant and positive relationship between attitudes and webcam covering behavior indicates that many users have solidified opinions on webcam covers which strongly impact their decision to use them.

We also find evidence that supports H2: the influence of subjective norms on behavior is highly significant in our research model. In fact, this means that when people in the social environment argue for a cover, users tend to follow their advice. This seems plausible as many users with a webcam cover stated that the reason for their use of the cover was a specific person's opinion about this topic (I16). Moreover, the feeling of embarrassment, which occurs among some users in situations where other people might spot their cover, impacts their adoption of webcam covering. Participants who are ashamed of covers and believe that others might think of themselves as paranoid are less likely to use one. This highlights that users with and without cover differ in their normative beliefs. While one group seems to perceive confirmation by their surrounding when covering the webcam, the other group thinks that using a cover is considered as strange behavior.

We find that perceived behavioral control has a highly significant impact on behavior, which supports H3. Thus, cover users are convinced to have more control over their privacy when deploying a cover. Specifically, they believe that covering the webcam protects them against spying attacks by foreign governments (PBC2). This is underlined by our finding that many users cover their webcam because of certain incidents they have heard of in the media (I16), such as the Snowden affair. Moreover, cover users intend to protect themselves from their own government (PB2C), criminals (PBC4), as well as Internet firms (PB5). In a relative sense, users are less likely to think that covers serve as a protection against spying attacks from people within their social environment. Independent of the attacker type, the vast majority of our participants believes that they would not be able to notice a webcam spying attack on their laptop (I18). We assume that this is caused by a lack of trust in the effectiveness of technologies that are supposed to inform them about malicious activities, such as the webcam indicator light or general software-based security measures.

Our analysis indicates that users' level of privacy concern does not significantly impact their webcam covering decision. In fact, more than half of the participants who stated to be highly concerned about their privacy were observed without a webcam cover. Thus, there is a discrepancy between users' level of concern and actual protective behavior. The significant impact of users' attitudes and subjective norms may explain why highly concerned users abstain from webcam covering: they are more likely to perceive a webcam cover as inconvenient, ugly, and embarrassing when it is visible to others.

To answer our initial research question, we can conclude from our empirical analysis that users' webcam covering behavior is influenced by their personal opinions, perceived opinions of their social environment, and the perception to have the ability to protect their privacy with a cover.

Theoretical Implications

Our results provide empirical evidence that the TPB can be used to explain why laptop users cover their webcams. To the best of our knowledge, only few previous studies investigate the link between attitude and actual privacy behavior, and some could not verify this relationship as they focus on user concerns. The results of our PLS analysis reveal that including

an additional construct for users' privacy concerns does not lead to an improvement of the model. Thus, we implicate that the constructs of the TPB need to be considered when investigating users' adoption of online privacy measures. Specifically, the approach to weight expectations with valuations is rarely used in empirical privacy research, but contributes to the validity of the findings. We recommend that follow-up studies take our findings into account when designing measurement instruments.

Our findings relate to the previously mentioned privacy paradox. Our analysis indicates that users' level of concern does not significantly impact their decision to cover the webcam. In fact, more than half of the participants who stated to be highly concerned did not cover their webcam. Even though, not using a webcam cover cannot directly be put on a level with users' active disclosure of personal data, the behavior studied when the paradox was established, we indeed find a discrepancy between users' level of concern over the risk of webcam spying and their actual protection behavior. But unlike in typical privacy paradox studies, we *can explain* this behavior with specific items measuring users' attitudes and subjective norms towards the protection measure. Users refrain from protection in particular if they perceive a webcam cover as impractical, ugly, and embarrassing when it is visible to others. Such specific factors were not considered in work establishing the privacy paradox, hence the TPB, along with its measurement principles, may resolve the apparent paradox. Of course, more studies in other contexts are needed for confirmation.

Practical Implications

As our results show that many laptop users make efforts to actively protect themselves from webcam spying attacks by manually adjusting the hardware of their computing devices, we suggest that the design of most built-in webcams does not sufficiently satisfy many users' privacy expectations. This leads them to accept the inconvenience caused by webcam covers. The confirmation of our proposed hypotheses shows that the perceived level of inconvenience varies among laptop users, whereas the level of concern over the risk of webcam spying does not play a decisive role. From these findings, we implicate that users' willingness to accept inconvenience as a trade-off for privacy is mainly influenced by their evaluation of subjectively perceived disadvantages and benefits of the respective privacy measure, and less by their risk evaluation. This highlights the importance of designing privacy enhancing technologies which are usable and less distracting for most users, since users' perceived level of inconvenience may substantially influence their decision to adopt.

It is certainly possible that the high proportion of users covering their webcams is because this privacy measure is intuitive, verifiably effective, and easy to copy from others. In fact, webcam covering is adopted by laptop users of most age groups, levels of education, and occupation types. This suggest that privacy measures which are socially accepted, and can be deployed effortlessly, are widely adopted, although the risk of losing privacy without these measures is deemed rather low. Designers of privacy enhancing technologies should keep these aspects in mind. Clearly, most software-based privacy measures are not as simple to deploy as webcam covering – but designers should develop strategies to enable users of all backgrounds to protect their privacy. Such efforts are barely wasted as our results show that users are willing to self-protect if they understand how to do it.

Our study indicates that if we want to incentivize users to cover their webcams, promoting social awareness and social desirability of the privacy protective measures may be the way to go. This suggestion can be derived from our result that perceived social norms significantly influence users' decision to protect their privacy. However, we cannot tell whether webcam covering is socially desirable: users have diverse utility functions comprising their individual perceived costs and benefits from adopting covering behavior, which add up to what economists call social welfare. Whether social welfare increases or decreases in case that the protective behavior gets promoted certainly is a topic for future research.

Limitations

It is important to point out that this study has some limitations. First, our sample is small and biased towards students (57%). This has two main reasons: first, the data was collected in a college town with a student share of around 20% of the population. Second, younger people are more likely to use a laptop [30]. Moreover, we are not able to draw conclusions about possible cultural differences regarding webcam covering behavior. Studies show that privacy concerns differ between cultures and may correlate with the privacy norms and laws in the respective countries [7, 51]. It is possible that cultural specificities and privacy regulations have an impact on the proportion of users with webcam covers, which should be taken into account for future research. Anecdotal evidence from discussing this research with international colleagues indicates that webcam covers are less prevalent in the USA than in Germany. The fact that our implications have a broader scope than the specific measure studied here as an example for observable privacy protection behavior puts these limitations into perspective.

CONCLUSION

This study is the first to investigate laptop users' webcam covering behavior by applying the Theory of Planned Behavior. Our field data collection at public places enabled us to unobtrusively observe this privacy protection behavior as a special kind of human-machine interaction. About a third of the study participants used a webcam cover on their laptop. A questionnaire was administered to collect additional data about personal characteristics of users with and without webcam cover. We use Partial Least Squares analysis to fit a latent factor path model to understand the drivers that lead users to adopt or abstain from covering their webcam. They perform this behavior largely independent of their stated level of privacy concerns, but rather because of specific beliefs regarding webcam covers. We find that users are heterogeneous in these beliefs. As a consequence, developers should take our results as a lesson on the importance of designing privacy enhancing technologies which are perceived as highly usable, intuitive, and easy to understand for most users.

ACKNOWLEDGMENTS

We thank Laura Schaffeld and Hanno Jenkel for helping with the data collection. We also thank the anonymous reviewers for helpful comments. This work received funding from the German Bundesministerium für Bildung und Forschung (BMBF) under grant agreement 16KIS0382 (AppPETs).

REFERENCES

1. Alessandro Acquisti. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the ACM Conference on Electronic Commerce (EC '04)*. ACM, New York, NY, USA, 21–29. DOI:http://dx.doi.org/10.1145/988772.988777
2. Alessandro Acquisti and Ralph Gross. 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International Workshop on Privacy Enhancing Technologies (PETS '06)*. Springer, Berlin Heidelberg, Germany, 36–58. DOI: http://dx.doi.org/10.1007/11957454_3
3. Icek Ajzen. 1985. *Action control: From cognitions to behaviors*. Springer, Berlin, Germany, Chapter From intentions to actions: A Theory of Planned Behavior, 11–39.
4. Icek Ajzen. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50, 2 (1991), 179–211. DOI: http://dx.doi.org/10.1016/0749-5978(91)90020-T
5. Icek Ajzen. 2002. Constructing a TPB questionnaire: Conceptual and methodological considerations. (2002). http://www-unix.oit.umass.edu/~aizen/pdf/tpb.measurement.pdf.
6. Susan B. Barnes. 2006. A privacy paradox: Social networking in the United States. *First Monday* 11, 9 (2006). DOI:http://dx.doi.org/10.5210/fm.v11i9.1394
7. Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society* 20, 5 (2004), 313–324. DOI: http://dx.doi.org/10.1080/01972240490507956
8. Brett Bilbrey. 2010. Embedded camera with privacy filter. U.S. Patent 7,728,906. (1 June 2010). Filed January 4, 2006.
9. Rainer Böhme and Stefanie Pötzsch. 2011. Collective exposure: Peer effects in voluntary disclosure of personal data. In *Financial Cryptography (FC '11)*. Springer, Berlin Heidelberg, Germany, 1–15.
10. Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347. DOI: http://dx.doi.org/10.1177/1948550612455931
11. Matthew Brocker and Stephen Checkoway. 2014. ISeeYou: Disabling the MacBook webcam indicator LED. In *Proceedings of the USENIX Security Symposium (USENIX Security '14)*. USENIX Association, Berkeley, CA, USA, 337–352. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/brocker
12. Barry Brown. 2001. Studying the Internet experience. (2001). http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.
13. Wynne W. Chin. 1998. *Modern methods for business research* (8th ed.). Lawrence Erlbaum Associates, Mahwah, NJ, USA, Chapter The partial least squares approach to structural equation modeling, 295–336.
14. Wynne W. Chin. 2010. *Handbook of partial least squares: Concepts, methods and applications*. Springer, Berlin, Germany, Chapter How to write up and report PLS analyses, 655–690.
15. James DeLong. 2011. Computer webcam privacy cover. U.S. Patent D643,457. (16 August 2011). Filed June 21, 2010.
16. Tamara Denning, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, and William H Maisel. 2010. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 917–926. DOI: http://dx.doi.org/10.1145/1753326.1753462
17. Lothar Determann and Robert Sprague. 2011. Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkeley Technology Law Journal* 26, 2 (2011), 979–1036. DOI:http://dx.doi.org/10.15779/Z38CQ5V
18. Alex Dobuzinskis. 2013. California man agrees to plead guilty to extortion of Miss Teen USA. (2013). https://www.reuters.com/article/us-usa-missteen-extortion/california-man-agrees-to-plead-guilty-to-extortion-of-miss-teen-usa-idUSBRE99U1G520131031.
19. Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens Le Blond, Damon McCoy, and Kirill Levchenko. 2017. To catch a ratter: Monitoring the behavior of amateur DarkComet RAT operators in the wild. (2017). DOI: http://dx.doi.org/10.1109/SP.2017.48
20. FBI. 2014. International Blackshades malware takedown. (2014). https://www.fbi.gov/news/stories/international-blackshades-malware-takedown-1.
21. Martin Fishbein and Icek Ajzen. 1975. *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley, Reading, MA, USA.
22. Jason Fitzpatrick. 2016. How to disable your webcam (and why you should). (2016). https://www.howtogeek.com/210921/how-to-disable-your-webcam,-and-why-you-should/.

23. Jens Fortmann. 2013. Closure device for an image capture facility. U.S. Patent 8,471,956. (25 June 2013). Filed October 29, 2010.

24. Seymour Geisser. 1974. A predictive approach to the random effect model. *Social Science Computer Review* 61, 1 (1974), 101–107. DOI: http://dx.doi.org/10.2307/2334290

25. Joey F. George. 2004. The Theory of Planned Behavior and Internet purchasing. *Internet Research* 14, 3 (2004), 198–212. DOI: http://dx.doi.org/10.1108/10662240410542634

26. Oliver Götz, Kerstin Liehr-Gobbers, and Manfred Krafft. 2010. *Handbook of partial least squares: Concepts, methods and applications*. Springer, Berlin, Germany, Chapter Evaluation of structural equation models using the partial least squares (PLS) approach, 691–711.

27. Ron G. Gustaveson. 2012. Webcam cover. U.S. Patent D669,112. (16 October 2012). Filed February 22, 2011.

28. Joseph F. Hair Jr., G. Tomas M. Hult, Christian Ringle, and Marko Sarstedt. 2016. *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications, Thousand Oaks, CA, USA.

29. Joseph F. Hair Jr., Christian M. Ringle, and Marko Sarstedt. 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice* 19, 2 (2011), 139–152. DOI:http://dx.doi.org/10.2753/MTP1069-6679190202

30. Horizont. 2014. Usage of consumer electronics in Germany, by age and device type. (2014). https://www.statista.com/statistics/448268/consumer-electronics-usage-by-device-type-and-age-germany/.

31. Chih-Min Huang, Yi-Ting Chen, and Li-Yen Wang. 2012. Laptop computer with hardware security protection. U.S. Patent 8,242,924. (14 August 2012). Filed September 16, 2009.

32. Thomas Hughes-Roberts and Elahe Kani-Zabihi. 2014. On-line privacy behavior: Using user interfaces for salient factors. *Journal of Computer and Communications* 2, 4 (2014), 220–231. DOI: http://dx.doi.org/10.4236/jcc.2014.24029

33. Ming-Chi Lee. 2009. Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications* 8, 3 (2009), 130–141. DOI: http://dx.doi.org/10.1016/j.elerap.2008.11.006

34. Younghwa Lee and Kenneth A. Kozar. 2005. Investigating factors affecting the adoption of anti-spyware systems. *Commun. ACM* 48, 8 (2005), 72–77. DOI:http://dx.doi.org/10.1145/1076211.1076243

35. Sonia Livingstone. 2008. Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10, 3 (2008), 393–411. DOI: http://dx.doi.org/10.1177/1461444808089415

36. May O. Lwin and Jerome D. Williams. 2003. A model integrating the multidimensional developmental Theory of Privacy and Theory of Planned Behavior to examine fabrication of information online. *Marketing Letters* 14, 4 (2003), 257–272. DOI: http://dx.doi.org/10.1023/B:MARK.0000012471.31858.e5

37. Dominique Machuletz, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2016. Users protect their privacy if they can: Determinants of webcam covering behavior. In *Proceedings of the European Workshop on Usable Security (EuroUSEC '16)*. Internet Society, Reston, VA, USA. DOI: http://dx.doi.org/10.14722/eurousec.2016.23014

38. Saeed Mirzamohammadi and Ardalan Amiri Sani. 2016. Viola: Trustworthy sensor notifications for enhanced privacy on mobile systems. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys '16)*. ACM, New York, NY, USA, 263–276. DOI: http://dx.doi.org/10.1145/2906388.2906391

39. Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126. DOI: http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x

40. Paul A. Pavlou and Lin Chai. 2002. What drives electronic commerce across cultures? Across-cultural empirical investigation of the Theory of Planned Behavior. *Journal of Electronic Commerce Research* 3, 4 (2002), 240–253.

41. Paul A. Pavlou and Mendel Fygenson. 2006. Understanding and predicting electronic commerce adoption: An extension of the Theory of Planned Behavior. *MIS quarterly* 30, 1 (2006), 115–143.

42. Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's watching me?: Assessing the effectiveness of webcam indicator lights. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1649–1658. DOI: http://dx.doi.org/10.1145/2702123.2702164

43. Peter Prüfer and Margrit Rexroth. 2005. Kognitive Interviews. (2005). http://nbn-resolving.de/urn:nbn:de:0168-ssoar-201470.

44. Andrew Raij, Animikh Ghosh, Santosh Kumar, and Mani Srivastava. 2011. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 11–20. DOI: http://dx.doi.org/10.1145/1978942.1978945

45. Ruby A. Rouse. 2012. Is someone watching you through your webcam? (2012). http://campatch.com/wpcontent/uploads/2012/05/CamPatch-AcademyStudy-on-Webcam-Hacking-Awareness-May2012.pdf.

46. Gaston Sanchez. 2013. PLS path modeling with R. (2013). https://pdfs.semanticscholar.org/3713/8910151616de6f122d0e757b55c81c8737e5.pdf.

47. Ashkan Soltani and Timothy B. Lee. 2013. Research shows how MacBook webcams can spy on their users without warning. (2013). https://www.washingtonpost.com/news/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/?utm_term=.9d68526f643c.

48. Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the ACM conference on Electronic Commerce (EC '01)*. ACM, New York, NY, USA, 38–47. DOI:http://dx.doi.org/10.1145/501158.501163

49. Mervyn Stone. 1974. Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society* 36, 2 (1974), 111–147.

50. Alan F. Westin. 1967. *Privacy and freedom*. Atheneum, New York, NY, USA.

51. Kuang-Wen Wu, Shaio Yan Huang, David C. Yen, and Irina Popova. 2012. The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior* 28, 3 (2012), 889–897. DOI: http://dx.doi.org/10.1016/j.chb.2011.12.008