Users Protect Their Privacy If They Can: Determinants of Webcam Covering Behavior

Dominique Machuletz*, Henrik Sendt†, Stefan Laube‡ and Rainer Böhme^x
*†‡*Department of Information Systems, Westfälische Wilhelms-Universität Münster, Germany*
Email: **D.Machuletz@uni-muenster.de,* †*H.S@uni-muenster.de,* ‡ *Stefan.Laube@uni-muenster.de*
^{x}*Department of Computer Science, Universität Innsbruck, Austria*
Email: Rainer.Boehme@uibk.ac.at

Abstract—**Most notebooks sold today come with a built-in webcam, placed above the screen to facilitate users' visual communication. What is intended to be a service seems to raise privacy concerns to some users, who may seek protection by covering the webcams of their devices. No matter how effective, this habit makes users' actual privacy protection behavior observable to researchers. This paper presents an application of the Theory of Reasoned Action to investigate determinants that lead users to cover their notebook webcams. It is based on an analysis of face-to-face interview data collected from 113 individuals who used their notebooks in public places, e. g., libraries, cafés, or trains. These users self-reported their attitudes and subjective norms towards webcam covers and privacy in general, while the actual covering behavior was observed and recorded by the interviewer. We estimate three logistic regression models to analyze the data. Our results indicate that attitudes towards webcam covers can explain actual covering behavior. Furthermore, we do not observe that participants' attitudes or subjective norms towards privacy have a manifest impact on the behavior.**

Index Terms—**Privacy, Usability, Actual Protection Behavior, Webcam Cover, Theory of Reasoned Action, Field Study**

1. Introduction

Undoubtedly, recent advances in information technology reduce users' actual and perceived control over their personal data [1]. Consequently, concerns about information privacy are rising [2]. Information privacy refers to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [3]. Hence, it is about the decision to transfer personal data to third parties. This decision was easy to make during the early stages of the digital revolution. At that time, data generating sensors in personal devices barely existed, and users had almost full control over the information stored in memories. Furthermore, the technical capabilities of vendors were limited, such that it was not easy for them to transfer and analyze mass data recorded by their products [4]. Today, users' devices have the capability to collect big quantities of personal data and send it into "the cloud" at negligible cost [2]. Furthermore, user-facing cybercrime [5] and mass data analysis by businesses [6] and governments are hot topics. If devices collect and distribute users' personal data without their explicit consent to others, we speak of privacy violations. Many users are concerned about such violations [7]. This motivates research on users' privacy protection behavior.

Several studies on users' privacy protection behavior use varying research methods. Some scholars try to investigate behavior based on self-reported data collected with questionnaires (e. g., [8], [9], [10]). However, the reliability of these results is limited, as self-reports may not always reflect actual user behavior [11]. This has led to a string of privacy studies that focus on privacy measures disclosed by users in laboratory experiments (e. g., [12], [13], [14]). The weakness of these studies is that the experimental setting may bias participants' behavior. Besides the well-known Hawthorne effect [15], privacy experiments face the particular difficulty of creating a credible stimulus for the risks of data sharing without crossing ethical boundaries. This motivates research on users' self-disclosed privacy protection behavior in public (e. g., [16], [17], [18]).

In the tradition of these latter studies, we investigate factors that lead users to cover their notebook lenses with a piece of tape or dedicated covers. Webcam covers are simple, user-understandable "mechanism" reducing the risk of falling victim to webcam spying attacks. According to a report published in June 2015 [19], they are commonly used among Internet users worldwide. As today's technological infrastructure enables users to access the Internet with notebooks from almost everywhere in the world, covering behavior must be observable at public places. This motivates us to conduct a study where we assess notebook webcam covering behavior of users at public places, coupled with a questionnaire to measure personal characteristics leading to

EuroUSEC '16, 18 July 2016, Darmstadt, Germany
Copyright 2016 Internet Society, ISBN 1-891562-45-2
http://dx.doi.org/10.14722/eurousec.2016.23014

this behavior. To the best of our knowledge, our study is the first to causally investigate webcam covering behavior.

The rest of this paper is structured as follows. We discuss relations of our approach to prior art and propose our research question in Section 2. Section 3 introduces our research method. We conduct our analysis in Section 4, and present its results in Section 5. A discussion of the results and study limitations in Section 6 precedes our conclusion in Section 7.

2. Related Work and Research Question

Scholars have investigated for long the relationship between users' privacy preferences and actual privacy protecting behavior. We briefly review prominent studies related to our work in Section 2.1. Thereafter, in Section 2.2, we put our approach to measure webcam covering behavior into context and derive our research model. The availability of data to apply this research model is conditioned on users' perceived risk of uncovered webcams, which we examine in Section 2.3. However, this risk may vary between users, motivating our research question proposed in Section 2.4.

2.1. Privacy Preferences vs. Actual Behavior

Many studies reveal discrepancies between users' privacy preferences and their actual privacy protection behavior. This is commonly referred to as the *privacy paradox*, a term defined by Norberg *et al.* [20] as "the difference between information actually provided [by users] as compared to a willingness to provide."

Diverse studies on users' privacy preferences and actual behavior on the Internet present evidence for the existence of a privacy paradox. All of these studies stand in the tradition of work by Spiekermann *et al.* [12], who conduct an experimental study to reason about the relationship between users' privacy preferences and disclosure behavior during online shopping. Their results indicate that many users disclose a lot of personal information regardless of their self-reported privacy concerns. Following the central idea proposed in [12], other scholars conduct similar studies, experimenting in scope. For instance, Tufekci [21] analyzes the relationship between privacy concerns and disclosing behavior of *Facebook* and *Myspace* users. They find that users' general online privacy concerns do not influence their information disclosure on online social networking sites. The studies in [22], [23], [24] yield similar results.

Other studies refute the hypothesis that there is a privacy paradox. For instance, the authors of [25], [26], [27], [28], [29], [30] all find correlations between social network users' privacy concerns and their behavior to introduce strict privacy settings. Dinev and Hart [10] analyze factors that influence users' information disclosure on online shopping websites. They find that a high level of perceived Internet privacy risk relates to a low willingness to provide personal information. Similarly, George [9] examines the relationship between users' purchasing behavior on the Internet and their privacy concerns when transacting with merchants. His work reveals that when users believe in the Internet's trustworthiness and their own ability to buy online, they are more likely to transact with merchants than those without these characteristics. Finally, one could argue that there is no paradox at all because stated attitudes are generally a weak predictor of actual behavior; even more so as many privacy studies do not strictly observe the "principle of compatibility" (see [31], [32], [33]) in their measurements.

2.2. Theoretical Classification and Research Model

Our study on webcam covering relates to the works presented in the previous section as it adopts commonly used constructs: users' attitudes and subjective norms towards privacy protection behavior. Attitudes towards a behavior reflect the degree to which a user has a favorable or unfavorable evaluation of the behavior. Subjective norms reflect the perceived social pressure to perform (or not to perform) the behavior in question [31].

The Theory of Reasoned Action (TRA) [34] and the Theory of Planned Behavior (TPB) [31] position both constructs in a broader context. The theories have in common that they assume users' attitudes and subjective norms to affect behavioral intention, influencing actual behavior. Their main difference is that the TPB adds the user's perceived behavioral control as a construct. Hence, the application of the TPB is reasonable when the behavior of interest is not under complete volitional control [32]. In contrast, the TRA is appropriate to analyze behavior that can fully be determined by users. A premise of our research is that webcam covering is under full volitional control of users and does not require specific skills or knowledge. Thus, we choose the TRA as the theoretical basis for our work.

Our research model for this study, based on the TRA, is depicted in Fig. 1. It comprises two constructs: attitudes towards privacy and webcam covers; and subjective norms towards privacy and webcam covers. We can neglect the intention construct provided for in the original TRA, as its measurement does not have a predictive value: the intention construct is dispensable if data on users' intentions and actual behavior are collected simultaneously (see [9], [35], [36]). Thus, in our model users' attitudes and subjective norms directly influence webcam covering.

In order to be able to apply our research model, we require data on users' covering behavior. Such behavior is conditioned on perceived risk of uncovered webcams.

2.3. Risk of Uncovered Webcams

Users seem to perceive a risk of webcam misuse, although the actual risk is deemed rather small. Webcam spying is usually enabled by users themselves, who unintentionally download and install a remote administration tools (RAT) on their devices. Prominent examples of these tools are the "Blackshades" malware and the spyware "DarkComet". Once a tool is installed, it can be exploited by the attackers who initially disseminated them. There are reported cases for *private hackers* using these tools in order to spy on users.[1] Additionally, it is conceivable that *firms* are actively involved in webcam spying, e. g., on their employees.[2] Moreover, there are indicators that *government agencies*, e. g., the US Federal Bureau of Investigation (FBI), circulate RATs in order to spy on their citizens.[3] In fact, the FBI Director's own use of a webcam cover indicates that spying on webcams may be a persistent threat.[4] However, we are not aware of any scientific evidence for real attacks. Overall, the privacy risk to consumers arising from uncovered webcams might be negligible compared to, e. g., browser-based network tracking as investigated in [37]. Nevertheless, users seem to perceive the small risk of webcam spying. For instance, this is confirmed by a study of Portnoff *et al.* [38], assessing the effectiveness of webcam indicator lights in communicating a webcam's recording to users by conducting a laboratory experiment. Among other things, they find that the majority of their study participants recognize the possibility of webcam spying attacks. Most of them would immediately cover their webcam if it unexpectedly indicated recording. However, users' perceived risk of uncovered webcams may vary. This motivates a privacy study on determinants that lead users to cover their webcams.

2.4. Research Question

The overall research question in this paper is:

> *"Which personal characteristics influence users' behavior to cover their notebook webcams ?"*

This question can be refined using the following two hypotheses that relate to our research model in Figure 1:

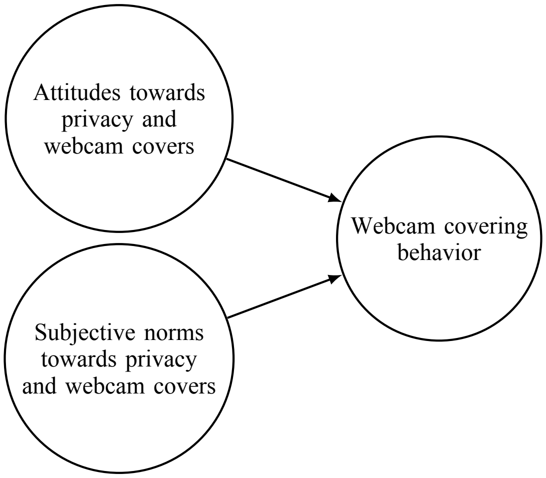
H1 Attitudes towards webcam covers and privacy significantly affect webcam covering behavior.

H2 Subjective norms towards webcam covers and privacy significantly affect webcam covering behavior.

3. Method

In order to answer the research question and to test the proposed hypotheses, we collected data by conducting a survey and observing participants' webcam covering behavior. We present the survey instrument in Section 3.1 and describe our survey procedure in Section 3.2.

Figure 1. Research Model Based on the TRA


Attitudes towards privacy and webcam covers
Subjective norms towards privacy and webcam covers
Webcam covering behavior

3.1. Instrument

Our instrument is designed to measure one dependent and two independent variables. The measurement of the dependent variable is presented in Section 3.1.1. Thereafter, in Section 3.1.2, we introduce the measurement and reliability scores of the two independent variables.

3.1.1. Dependent Variable. Webcam covering behavior is the dependent variable in our model. This variable does not have to be reported by participants, but is unobtrusively observed by the interviewer once users agree to participate in the study.

3.1.2. Independent Variables. The study's two independent variables concern participants' attitudes and subjective norms. Both have to be self-reported by participants. They are regarded as constructs measured *reflectively* with multiple items on seven-point rating scales, anchored at 1 (fully disagree) and 7 (fully agree). The measurement of all items is performed in German, with original wording reported in Table 5 (in the Appendix).

The attitudes construct consists of 12 items (Cronbach's $\alpha = 0.76$). We use 7 items for measuring attitudes towards webcam covers (Cronbach's $\alpha = 0.84$), asking participants about their subjective perceptions and opinions that relate to this privacy protecting behavior. Furthermore, 5 items are used to measure attitudes towards privacy (Cronbach's $\alpha = 0.46$), focusing on personal beliefs and perceptions regarding privacy preserving behavior, as well as opinions about privacy related topics.

The subjective norms construct consists of 8 items (Cronbach's $\alpha = 0.44$). We use 4 items to measure subjective norms towards webcam covers (Cronbach's $\alpha = 0.52$). Related questions ask for participants' perceptions how their social environment regards webcam covering. Moreover, we use 4 items for measuring subjective norms towards privacy (Cronbach's $\alpha = 0.37$), investigating participants' perceptions on how others regard information privacy.

[1] See, e. g., http://www.bbc.com/news/technology-34475151 and http://stoplooking.net/how-the-fbi-found-miss-teen-usas-webcam-spy/.

[2] This is, for instance, mentioned in http://www.huffingtonpost.com/rebecca-abrahams/your-computer--phone-came_b_5398896.html.

[3] See http://www.dailymail.co.uk/news/article-2520707/FBI-spy-webcam-triggering-indicator-light.html for further information.

[4] During a speech in Ohio, USA, FBI Director James Comey pointed out that he uses a webcam covers on his own laptop. See https://nakedsecurity.sophos.com/2016/04/12/why-the-fbi-director-puts-tape-over-his-webcam-and-you-should-too/.

3.2. Procedure

Our data collection took place in October 2015. We interviewed users of notebooks with webcams at different libraries, trains, canteens and cafés in and around Münster, a college town in Germany. Everyone who used a notebook with a webcam in public has been considered a potential study participant. We asked candidates whether they would like to take part in a research project dealing with notebook usage behavior. In this context, we informed them about the expected duration as well as the voluntary nature of participation in our study. Furthermore, we guaranteed anonymity. Once a candidate agreed, we handed out our survey on paper and secretly recorded his webcam covering behavior. On average, it took study participants about 4–5 minutes to complete the questionnaire. Subjects were debriefed after they took the survey. This included informing them on our recordance of webcam covering behavior.

4. Analysis

Our data analysis is based on $n = 113$ study participants. Their demographics, depicted in Table 1, are presented in Section 4.1. Thereafter, in Section 4.2, we propose the statistical model used to analyze the data.

4.1. Descriptive Analysis

By discussing the survey demographics we can give some intuition on how widespread the use of webcam covers is among different groups of study participants.

In total, 32% of all participants had a webcam cover.

Our sample contains more male (61%) than female (37%) participants, and is biased towards people aged between 18 and 29 (81%). One reason for this bias may be that the town where the data has been collected is small in comparison to its number of students.[5]

Of all female participants, we observe that nearly half had a webcam cover (43%). By contrast, only about one quarter (26%) of all males covered their webcams. We use Pearson's chi-squared test to assess differences between these two groups. The hypothesis that webcam covering behavior is independent of gender can be rejected with a significance level of 10% ($\chi^2 = 3.35$, $df = 1$, $p = 0.067$).

Of all young participants, about one third (32%) covered their webcam. We assume that younger people are in general more likely to cover their webcams than older ones. This is because younger generations grow up using information technology, and thus might develop an instinct regarding threats to their devices. Though, we cannot evaluate this assumption as the remaining age groups in our sample are too small to statistically test differences in webcam covering customs.

The demographics suggest that a considerable amount of participants (12%) make use of webcam covers even though they use their notebook for less than one hour a day. If participants indicate to have the habit of using their notebooks for longer than one hour a day, they are more likely to make use of webcam covers. Specifically, about a third of these participant (36%) covered their webcam on average. We use Pearson's chi-squared test to assess behavioral differences between the two notebook usage types. The hypothesis that webcam covering behavior is independent of notebook usage per day can be rejected with a significance level of 5% ($\chi^2 = 3.82$, $df = 1$, $p = 0.050$). An explanation may be that participants who use their notebook more frequently are better informed about potential risks, and therefore more likely to take precautionary measures.

Table 1. Survey Demographics

	Frequency (#)	Of all (%)	With cover (%)
Total	113	100.0	31.9
Gender			
Male	69	61.1	26.1
Female	42	37.2	42.9
Unknown	1	0.9	0.00
Age			
< 18	6	5.3	33.3
$18 - 29$	92	81.4	31.5
$30 - 39$	4	3.5	50.0
$40 - 49$	2	1.8	50.0
$50 - 59$	9	8.0	22.2
> 59	0	0.0	0.0
Notebook usage per day (hours)			
< 1	17	15.0	11.8
$1 - 2$	24	21.2	29.2
$3 - 4$	27	23.9	44.4
$5 - 6$	13	11.5	38.5
> 6	31	27.4	32.3
Webcam usage during last month (times)			
0	63	55.8	31.8
$1 - 4$	38	33.6	26.3
$5 - 8$	5	4.4	80.0
> 8	7	6.2	28.6
Antivirus installed			
Yes	98	86.7	31.6
No	15	13.3	33.3
Mobile phone front camera covered			
Yes	3	2.7	66.7
No	103	91.2	28.2
Use of mobile phone privacy filter			
Yes	7	6.2	57.1
No	103	91.2	31.1

Some variables have missing values.

In total, the majority of participants in our sample (56%) reported that they did not use their webcams at all during the past month. Nevertheless, about one third of these participants (32%) uses a webcam cover, regardless. However, based on our data, a causal link between the frequency of webcam usage and webcam covering behavior cannot be established.

Additionally, we can investigate relationships between participants' webcam covering behavior and their use of other security or privacy measures. We cannot find any correlation between covering behavior and used security measures, such as antivirus software. Furthermore, of all participants with a webcam cover in place (32%), most

[5] In the most recent demographics of Münster from 2014, the town had about $300,000$ residents. Simultaneously, about $45,000$ students were registered at the local university.

Table 2. Regression with All Items

Item code	Item description	Estimate	Exp. Estimate	Std. error	z value	Pr(>|z|)
(Intercept)		-5.76	0.00	3.89	-1.48	0.138
Attitudes towards webcam covers						
AW1	Fear of unauthorized webcam access	1.52	4.57	2.29	0.66	0.507
AW2	Opinion that one should protect from unauthorized webcam access	-2.45	0.09	2.33	-1.05	0.294
↔AW3	Perception that webcam covering is excessively cautious	0.12	1.12	2.28	0.05	0.960
AW4	**Perception that webcam covers are practical**	5.32	204.24	2.12	2.51	0.012 *
AW5	Perception that webcam covers are useful	-0.82	0.44	3.23	-0.25	0.800
AW6	**Perception that webcam covers are necessary**	7.18	1311.15	2.30	3.13	0.002 **
AW7	Perception that webcam covers are secure	1.04	2.82	2.24	0.46	0.643
Attitudes towards privacy						
↔AP1	Opinion that video cameras should be used at public places to increase security	-0.28	0.75	2.14	-0.13	0.895
↔AP2	Perception that the disclosure of own personal information in social networks is harmless	-3.25	0.04	2.91	-1.12	0.264
↔AP3	Willingness to upload a personal video on a public website	-0.85	0.43	2.52	-0.34	0.737
↔**AP4**	**Belief that the government sufficiently protects personal privacy on the Internet**	-6.31	0.00	3.18	-1.99	0.047 *
↔**AP5**	**Belief that firms respect personal privacy**	4.91	135.80	2.31	2.12	0.034 *
Subjective norms towards webcam covers						
SW1	**People in the social environment use a webcam cover**	-7.63	0.00	3.24	-2.35	0.019 *
SW2	**People in the social environment argue for webcam covering**	10.23	27758.95	3.90	2.62	0.009 **
SW3	Expectation of others to use a webcam cover in the work environment	2.70	14.89	2.12	1.27	0.203
↔SW4	Fear that others rate webcam covering overly cautious	-0.83	0.43	2.42	-0.34	0.731
Subjective norms towards privacy						
SP1	Perception that society expects Internet privacy self-protection	-3.45	0.03	1.87	-1.84	0.065
SP2	Privacy protection is an important topic in the social environment	1.01	2.76	2.02	0.50	0.614
↔SP3	Fear of social rejection for not being active in social networks	1.73	5.65	2.42	0.72	0.474
↔SP4	Fear of social rejection for not sharing pictures in social networks	-6.26	0.00	4.08	-1.54	0.125

Scales of items indicated by “↔” were reversed before conducting the analyses in Section 5.2 and Section 5.3
Significance level codes: 1% ’**’, 5% ’*’
Nagelkerkes’ pseudo-$R^2 = 0.74$

did not cover their mobile phone front camera (88%). By contrast, of all participants who indicated to cover their mobile phone front camera (3%), most had a webcam cover in place (67%). We also asked all participants if they use mobile phone privacy filters. Of the few study participants who used filters (6%), a considerable share (57%) also covered their notebook webcam.

We closed our questionnaire with two open questions. First, we asked participants with a webcam cover in place for how long they have been covering. Most of them (75%) answered that they cover their webcam for longer than one year. Second, we asked participants without a webcam cover regarding their covering behavior in the past. Surprisingly, some participants (17%) revealed that they once used a cover. A considerable amount of these participants (62%) stated a loss of the cover or the purchase of a new notebook as reasons for a change in behavior. Others (38%) mentioned that impracticability or poor outer appearance of webcam covers lead them to discontinue covering.

4.2. General Statistical Model

For an investigation of the relation between our independent and dependent variables, we compute logistic regressions. This is possible because our dependent variable is binary (webcam covered/not covered) and the independent variables are based on parametric measures. Thus, we may estimate the parameter vector $\hat{b} = \left(\hat{b}_0, \hat{b}_1, ...\right)$ using the following equation per response record to derive results considering all items:

$$\overbrace{\log\left(\frac{p}{1-p}\right)}^{\text{Behavior}} = b_0 + \overbrace{b_1 D_1 + ... +}^{\text{Attitudes}} \overbrace{b_i D_i + ...}^{\text{Subjective norms}} + \epsilon \ ,$$

where

- the dependent variable p is the probability for a participant to use a webcam cover,
- b_0 is a constant intercept,
- $(D_1, ..., D_{i-1})$ are values derived from questions on the participant’s attitudes,
- $(D_i, ...)$ are values derived from questions on the participant’s subjective norms,
- and ϵ is an error term reporting the difference between the true relationship and the model.

However, not every participant answered all questions. Thus, we need to handle missing values before conducting our analyses. We use the policy to discard response records from the data set if more than two values are missing. Otherwise, we fill in missing values by mean value imputation. Overall, our data set includes 22 records with missing values. Of these records, 13 are deleted based on our policy. Consequently, means are imputed for missing values in the other 9 records. Descriptive statistics for the influence of specific indicators based on the remaining $n = 100$ data records are provided in Table 6 (in the Appendix). This set of data records is used to compute our regression results. In order to estimate $\hat{b}$ with the maximum likelihood method, we use the implementation provided by the survey extension for R [39].

5. Results

We present results derived by the general statistical model in Section 5.1. This model can be adopted to two aggregate models, whose analysis enables us to reason on the impact of participants' overall attitudes and subjective norms. Corresponding adoptions and results are presented in Section 5.2 and Section 5.3. Tables 2–4 display the estimated coefficients $\hat{b}$ along with the exponentiated coefficients $e^{\hat{b}}$, standard errors, z-statistics, associated p-values and significance levels of the three different models. Each presented coefficient provides an indicator for the impact of a change in the log odds ratio of the dependent variable. Note that only the sign and magnitude of logistic regressions' coefficients can readily be interpreted, while actual values are not always intuitive. A positive coefficient denotes that – after controlling for all other variables in the model – an answer to the item within the upper half of the rating scale increases the likelihood of notebook webcam covering, and vice versa.

5.1. Regression with All Items

Table 2 depicts the results for the statistical model presented in Section 4.2. Our model specification explains about 74% of the variation in the dependent variable.

We observe three characteristics that have a significant and positive impact on participants' webcam covering behavior. First, participants' perception that webcam covers are practical (AW4) leads them towards covering their webcam. This finding goes in line with answers to the second of our open-ended questions in the questionnaire: impracticability is one of the reported reasons for participants to stop using webcam covers. Second, participants' perception that webcam covers are necessary (AW6) has a positive impact on covering behavior. As we did not ask for the root causes of this perception, we may assume that necessity is perceived because of (reports of) experiences with webcam hacks in the past. Another explanation could be social pressure. This would go in line with our third observation: if people in the social environment of a participant argue for the use of webcam covers (SW2), this has a positive impact on behavior adoption.

However, this last result lets another finding appear to be puzzling: participants' observation that others in their social environment use webcam covers (SW1) has a significant and negative impact on the adoption of this behavior. A quick look at the descriptive statistics in Table 6 (in the Appendix) reveals that the sign of the estimated coefficient of SW1 points in the opposite direction as suggested by the difference in means. This indicates a suppression effect [40]. In fact, if the logistic regression is computed based on the general model but omitting SW2, we find that SW1 becomes insignificant. Thus, SW1 is suppressed by SW2. This indicates that webcam covers are issues discussed in the social environment of some participants. Moreover, partisanship for and actual use of webcam covers are obviously not independent.

Table 3. Regression with Items Condensed to Four Variables

		Exp.	Std.			
	Estimate	Estimate	Error	z value	Pr(>|z|)	
(Intercept)	-9.49	0.00	2.55	-3.72	0.000	***
Attitudes towards webcam covers	7.20	1343.99	1.86	3.86	0.000	***
Attitudes towards privacy	3.02	20.49	2.38	1.27	0.205	
Subjective norms towards webcam covers	3.41	30.12	1.87	1.82	0.068	
Subjective norms towards privacy	-0.11	0.90	1.82	-0.06	0.952	

Significance level code: 0.1% '***'
Nagelkerkes' pseudo-$R^2 = 0.46$

Furthermore, we observe one characteristic that leads participants to abstain from webcam covering. Our results show that participants' belief that governments sufficiently protects their Internet privacy (AP4) has a significant and negative impact on webcam covering behavior. This result is intuitive and pronounces the role of governments regarding users' privacy protection.

By contrast to the previous result, participants' belief that firms respect personal privacy (AP5) has a positive impact on behavior adoption. This result is somewhat surprising, as webcam covering indicates distrust. Table 6 (in the Appendix) reveals that the estimated coefficient of AP5 points in the opposite direction as suggested by the descriptives, signaling a second suppression effect. A closer investigation reveals that AP4 suppresses AP5. A logistic regression computed omitting AP4 lets AP5 become insignificant. This may indicate that some webcam users differentiate between threats and the specific effectiveness of webcam covers: those who cover their lenses mainly for distrust against government spies may be aware that this behavior is of little help against commercial tracking.

Overall, the observed suppression effects indicate that our instrument should be refined in follow-up studies, e. g., by adding more direct items on the perceived effectiveness of webcam covers against specific threats, or by exploring the role of visible covers on personal devices as political statements. Future studies should also include a wider range of questions about trust/distrust in other types of possible attackers (e. g. relating to private attackers).

5.2. Regression with Four Variables

In this section, we estimate the parameter vector $\hat{b} = \left(\hat{b}_0, \hat{b}_1, \hat{b}_2, \hat{b}_3, \hat{b}_4\right)$ after we condense all data items to four variables $(\bar{D}_1, \bar{D}_2, \bar{D}_3, \bar{D}_4)$: attitudes towards webcam covers, attitudes towards privacy, subjective norms towards webcam covers, and subjective norms towards privacy. Note that we have to reverse some item scales (depicted by a “$\leftrightarrow$” in Table 2) to derive meaningful mean values. For instance, the scaling of the item “AP1 Opinion that video cameras should be used at public places to increase security” has to be reversed as answers in the lower rather than the upper half of the rating sale indicate attitudes towards privacy. After computing the regression results, we are able to reason which of the four variables can best explain webcam covering behavior.

This model specification explains 46% of the variation in the dependent variable, as depicted in Table 3. We observe that only attitudes towards webcam covers have a strong and significant positive impact on webcam covering behavior. Attitudes towards privacy and subjective norms do not predict behavior at all. Thus we cannot confirm that privacy aware participants are likely to cover their webcams, or society at large has an impact on this behavior.

5.3. Regression with Two Variables

We may also estimate the parameter vector $\hat{b} = \left(\hat{b}_0, \hat{b}_1, \hat{b}_2\right)$ after we condense all item data to two variables $(\bar{D}_1, \bar{D}_2)$: attitudes towards webcam covers and privacy, and subjective norms towards webcam covers and privacy. Again, we have to reverse some item scales to conduct a meaningful analysis, following the rationale proposed in the last Section. The resulting $\hat{b}$, derived by the maximum likelihood method, enable us to answer our hypotheses posed in Section 2.4.

This model specification explains 43% of the variation in the dependent variable, as depicted in Table 4. The regression results indicate that attitudes towards webcam covers and privacy have a strong and significant positive impact on webcam covering behavior. In contrast, subjective norms do not predict the behavior at all.

6. Discussion

After analyzing the data and reporting of associated results, we can now revisit the hypotheses proposed in Section 2.4.

H1 *Supported for attitudes towards webcam covers*
H2 *Not supported*

Regarding H1, we find that participants with an attitudes towards webcam covers and privacy are more likely to use a notebook webcam cover than others. Based on our regression analyses, we can conclude that predominantly attitudes towards webcam covers have a positive impact on behavior. Specifically, participants’ perceived practicability and necessity of covers leads them to adapt covering behavior.

Table 4. Regression with Items Condensed to Two Variables

	Estimate	Exp. Estimate	Std. Error	z value	Pr(>|z|)	
(Intercept)	-11.05	0.00	2.37	-4.66	0.000	***
Attitudes towards webcam covers and privacy	11.82	135537.01	2.89	4.09	0.000	***
Subjective norms towards webcam covers and privacy	3.39	29.78	2.53	1.34	0.180	

Significance level code: 0.1% ’***’
Nagelkerkes’ pseudo-$R^2 = 0.43$

Contrary to our expectation, the results also indicate mixed findings on whether privacy preferences have a significant and positive impact on webcam covering.

With respect to H2, we do not find evidence that subjective norms towards webcam covers and privacy significantly affect covering behavior. This may be explained by the low internal consistency of the corresponding items. Acknowledging the results in Section 5.1, we find that participants’ behavior is influenced by people in their social environment who use a webcam cover and argue for it.

In general, we observe that females cover their webcams more often than males, and that covering behavior depends on users’ notebook usage per day. Future research should strive to rule out the potential effect of third variables driving these headline results. No causal relationship can be found between covering behavior and the frequency of webcam usage or the use of notebook security measures.

Our study has a number of limitations. First, we have a selection bias. Our recruitment procedure seeks interviews with users who use notebooks in public only, excluding those who use their devices at home or at work. Those are environments where the expectation of privacy might be even higher and people may use different devices. Second, some reliability scores of our questionnaire are rather weak, as discussed in Section 3.1. Third, our models in Section 5.2 and Section 5.3 have a fairly weak fit. Because of these last two limitations, the corresponding results have to be interpreted with caution. In general, we suggest that future investigations also take different constructs into consideration and refine the item batteries in the questionnaire. We see considerable potential for further research on webcam covering behavior and consider this work a preliminary study, mainly to explore and structure the use of a novel and interesting indicator of actual privacy protection behavior.

7. Conclusion

Portable devices with integrated webcams bring numerous benefits to users. They are convenient to use, enable face-to-face communication over the Internet, serve as barcode scanners, etc. Unfortunately, these devices also raise privacy concerns. This is because cybercriminals can hijack them and blackmail victims with obtained footage, vendors may collect data via the devices for their own economic advantage, and governments can take over webcams as part of their missions to combat organized crime and terrorism. Thus, many users choose to forgo some of the benefits of webcams and cover their notebook lenses with a piece of tape or even dedicated covers available on the market.

To the best of our knowledge, we present the first empirical analysis that tries to shed light into users' webcam covering behavior. Our results indicate that attitudes towards webcam covers have a positive impact on the use of covers. Specifically, participants who perceive covers as necessary or practical adopt this behavior. Furthermore, we do not find evidence that attitudes or subjective norms towards privacy have a measurable impact on covering behavior.

More than 30% of the participants of our convenience sample do use a webcam cover. This not only provides a useful indicator of actual privacy protection behavior for empirical research. It also gives rise to optimism that users take action to protect their privacy

- if the measure is simple,
- perceived as effective,
- and socially acceptable.

Developers of privacy enhancing technologies (PETs) should take this as a lesson on the value of usability. They should try to copy the success factors of this hardware gadget to the truly effective software-based protection mechanisms they design.

Acknowledgments

The authors acknowledge the help of Severin Hußmann and Hanno Jenkel in collecting the survey data and for their contributions to the data analysis. Furthermore, they thank all study participants for their time.

References

[1] E. A. Whitley, "Informational privacy, consent and the 'control' of personal data," *Information Security Technical Report*, vol. 14, no. 3, pp. 154–159, 2009.

[2] J. van den Hoven, M. Blaauw, W. Pieters, and M. Warnier, "Privacy and information technology," in *The Stanford Encyclopedia of Philosophy*, Spring 2016 ed., E. N. Zalta, Ed., 2016.

[3] A. F. Westin, *Privacy and freedom*, 1st ed. New York, NY, USA: Atheneum, 1967.

[4] A. R. Miller, "Personal privacy in the computer age: The challenge of a new technology in an information-oriented society," *Michigan Law Review*, vol. 67, no. 6, pp. 1089–1246, 1969.

[5] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *The Economics of Information Security and Privacy*, R. Böhme, Ed. Berlin, Heidelberg, Germany: Springer, 2013, ch. 12, pp. 265–300.

[6] R. van der Meulen and V. Woods, "Gartner survey shows more than 75 percent of companies are investing or planning to invest in big data in the next two years," Tech. Rep., 2015.

[7] R. A. Rouse, "Is someone watching you through your webcam?" Tech. Rep., 2012.

[8] F. Stutzman and J. Kramer-Duffield, "Friends only: Examining a privacy-enhancing behavior in facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, New York, NY, USA, 2010, pp. 1553–1562.

[9] J. F. George, "The theory of planned behavior and internet purchasing," *Internet research*, vol. 14, no. 3, pp. 198–212, 2004.

[10] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006.

[11] I. Ajzen, C. Timko, and J. B. White, "Self-monitoring and the attitude–behavior relation." *Journal of Personality and Social Psychology*, vol. 42, no. 3, pp. 426–435, 1982.

[12] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior," in *Proceedings of the 3rd ACM conference on Electronic Commerce (EC)*, New York, NY, USA, 2001, pp. 38–47.

[13] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, vol. 48, no. 4, pp. 101–106, 2005.

[14] A. R. Beresford, D. Kübler, and S. Preibusch, "Unwillingness to pay for privacy: A field experiment," *Economics Letters*, vol. 117, no. 1, pp. 25–27, 2012.

[15] F. J. Roethlisberger and W. J. Dickson, *Management and the worker: An account of a research program conducted by the Western electric Company, Hawthorne Works, Chicago*, 14th ed. Cambridge, MA, USA: Harvard University Press, 1939.

[16] T. Hughes-Roberts, "Privacy and social networks: Is concern a valid indicator of intention and behaviour?" in *2013 International Conference on Social Computing (SocialCom)*, Washington, DC, USA, 2013, pp. 909–912.

[17] K. Lewis, J. Kaufman, and N. Christakis, "The taste for privacy: An analysis of college student privacy settings in an online social network," *Journal of Computer-Mediated Communication*, vol. 14, no. 1, pp. 79–100, 2008.

[18] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society (WPES)*, Alexandria, VA, USA, 2005, pp. 71–80.

[19] Kaspersky Lab; B2B International, "Actions to protect devices and online usage privacy according to internet users worldwide as of June 2015," Tech. Rep., 2015.

[20] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[21] Z. Tufekci, "Can you see me now? Audience and disclosure regulation in online social network sites," *Bulletin of Science, Technology & Society*, vol. 28, no. 1, pp. 20–36, 2008.

[22] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, 2006.

[23] M. Taddicken, "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure," *Journal of Computer-Mediated Communication*, vol. 19, no. 2, pp. 248–273, 2014.

[24] B. Reynolds, J. Venkatanathan, J. Gonçalves, and V. Kostakos, "Sharing ephemeral information in online social networks: Privacy perceptions and behaviours," in *Human-Computer Interaction (INTERACT)*, Lisbon, Portugal, 2011, pp. 204–215.

[25] S. Utz and N. Krämer, "The privacy paradox on social network sites revisited: The role of individual characteristics and group norms," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 3, no. 2, pp. 1–10, 2009.

[26] G. Blank, G. Bolsover, and E. Dubois, “A new privacy paradox: Young people and privacy on social network sites,” in *Annual meeting of the American Sociological Association (ACA)*, vol. 17, San Francisco, CA, USA, 2014.

[27] A. L. Young and A. Quan-Haase, “Privacy protection strategies on facebook: The internet privacy paradox revisited,” *Information, Communication & Society*, vol. 16, no. 4, pp. 479–500, 2013.

[28] E. Christofides, A. Muise, and S. Desmarais, “Information disclosure and control on facebook: Are they two sides of the same coin or two different processes?” *Cyberpsychology & Behavior: The impact of the internet, multimedia and virtual reality on behavior and society*, vol. 12, no. 3, pp. 341–345, 2009.

[29] C. Lutz and P. Strathoff, “Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses,” in *Multinationale Unternehmen und Institutionen im Wandel - Herausforderungen für Wirtschaft, Recht und Gesellschaft*, 1st ed. Bern, Switzerland: Stämpfli Verlag, 2013, ch. 8, pp. 81–99.

[30] T. Dienlin and S. Trepte, “Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors,” *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[31] I. Ajzen, “The theory of planned behavior,” *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, 1991.

[32] ——, *Attitudes, personality, and behavior*. Homewood, IL, US: Open University Press, 1988.

[33] S. Sutton, “Predicting and explaining intentions and behavior: How well are we doing?” *Journal of Applied Social Psychology*, vol. 28, no. 15, pp. 1317–1338, 1998.

[34] M. Fishbein and I. Ajzen, *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA, USA: Addison-Wesley, 1975.

[35] I. Ajzen and M. Fishbein, *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ, USA: Prentice Hall, 1980.

[36] D. M. Randall and J. A. Wolff, “The time interval in the intention-behaviour relationship: Meta-analysis,” *British Journal of Social Psychology*, vol. 33, no. 4, pp. 405–418, 1994.

[37] S. Engelhardt and A. Narayanan, “Online tracking: A 1-million-site measurement and analysis,” Tech. Rep., 2016.

[38] R. S. Portnoff, L. N. Lee, S. Egelman, P. Mishra, D. Leung, and D. Wagner, “Somebody’s watching me?: Assessing the effectiveness of webcam indicator lights,” in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*, Seoul, Republic of Korea, 2015, pp. 1649–1658.

[39] R Core Team, “R: A language and environment for statistical computing,” Vienna, Austria, Tech. Rep., 2013. [Online]. Available: http://www.R-project.org/

[40] D. P. MacKinnon, J. L. Krull, and C. M. Lockwood, “Equivalence of the mediation, confounding and suppression effect,” *Prevention Science*, vol. 1, no. 4, pp. 173–181, 2000.

Appendix

Table 5. Original Question Wording

Item code	Item
Attitudes towards webcam covers	
AW1	Ich habe Angst, dass jemand unautorisiert auf meine Webcam zugreifen kann
AW2	Ich bin der Meinung, man sollte sich vor unautorisiertem Zugriff auf die eigene Webcam schützen
AW3	Ich erachte das Abdecken der Webcam als eine übertriebene Vorsichtsmaßnahme
AW4	Ich halte Webcam-Abdeckungen für praktisch
AW5	Ich halte Webcam-Abdeckungen für nützlich
AW6	Ich halte Webcam-Abdeckungen für notwendig
AW7	Ich halte Webcam-Abdeckungen für sicher
Attitudes towards privacy	
AP1	Ich bin der Meinung, Videokameras sollten an öffentlichen Orten eingesetzt werden, um die allgemeine Sicherheit zu steigern
AP2	Ich halte es für unbedenklich, persönliche Informationen über mich auf sozialen Netzwerken (wie z. B. *facebook*) preis zu geben
AP3	Ich würde ein Video von mir auf einer öffentlich zugänglichen Webseite hochladen
AP4	Ich glaube, dass der Staat meine Privatsphäre im Internet ausreichend schützt
AP5	Ich glaube, dass Unternehmen meine Privatsphäre respektieren
Subjective norms towards webcam covers	
SW1	Viele Leute in meinem Umfeld decken ihre Webcam ab
SW2	Viele Leute in meinem Umfeld sind der Meinung, ich sollte meine Webcam abdecken
SW3	Es wird in meinem Arbeitsumfeld von mir erwartet, dass ich meine Webcam abdecke
SW4	Ich befürchte, dass meine Umwelt mich für übertrieben vorsichtig hält, wenn ich meine Webcam abklebe
Subjective norms towards privacy	
SP1	Ich denke, es wird gesellschaftlich von mir erwartet, meine Privatsphäre selbst im Internet zu schützen
SP2	In meinem Umfeld ist der Schutz der Privatsphäre ein wichtiges Thema
SP3	Ich befürchte Ablehnung seitens meines Umfelds, wenn ich nicht in sozialen Netzwerken (wie z. B. *facebook*) aktiv bin
SP4	Ich befürchte Ablehnung seitens meines Umfelds, wenn ich keine Bilder von mir in sozialen Netzwerken (wie z. B. *facebook*) teile
Additional open questions	
AQ1	Falls Sie Ihre Webcam momentan abgedeckt haben, wie lange ist dies bereits der Fall?
AQ2	Falls Sie Ihre Webcam am Laptop momentan nicht abgedeckt haben, haben Sie dies in der Vergangenheit getan? Wenn ja, wieso ist dies nicht mehr der Fall?

Table 6. Descriptive Statistics for All Items

Item code	Item description	Total $(n = 100)$		With cover $(n = 32)$		Without cover $(n = 78)$	
		Mean	SD	Mean	SD	Mean	SD
Attitudes towards webcam covers							
AW1	Fear of unauthorized webcam access	4.09	1.75	4.59	1.72	3.85	1.73
AW2	Opinion that one should protect from unauthorized webcam access	5.13	1.58	5.53	1.59	4.94	1.55
AW3	Perception that webcam covering is excessively cautious	3.42	1.76	2.34	1.68	3.93	1.58
AW4	**Perception that webcam covers are practical**	**4.27**	**1.98**	**5.56**	**1.48**	**3.67**	**1.90**
AW5	Perception that webcam covers are useful	5.33	1.65	6.38	0.75	4.84	1.73
AW6	**Perception that webcam covers are necessary**	**4.55**	**1.90**	**6.16**	**1.25**	**3.79**	**1.67**
AW7	Perception that webcam covers are secure	5.61	1.47	6.06	1.13	5.40	1.57
Attitudes towards privacy							
AP1	Opinion that video cameras should be used at public places to increase security	4.06	1.76	3.78	1.64	4.19	1.81
AP2	Perception that the disclosure of own personal information in social networks is harmless	2.46	1.42	1.97	0.82	2.69	1.58
AP3	Willingness to upload a personal video on a public website	2.58	1.60	2.16	1.32	2.78	1.68
AP4	**Belief that the government sufficiently protects personal privacy on the Internet**	**2.31**	**1.18**	**2.12**	**1.13**	**2.40**	**1.20**
AP5	**Belief that firms respect personal privacy**	**2.36**	**1.40**	**2.31**	**1.38**	**2.38**	**1.43**
Subjective norms towards webcam covers							
SW1	**People in the social environment use a webcam cover**	**4.70**	**1.71**	**5.03**	**1.53**	**4.54**	**1.77**
SW2	**People in the social environment argue for webcam covering**	**3.57**	**1.70**	**4.42**	**1.60**	**3.18**	**1.61**
SW3	Expectation of others to use a webcam cover in the work environment	1.92	1.29	2.59	1.34	1.60	1.15
SW4	Fear that others rate webcam covering overly cautious	2.62	1.37	2.53	1.24	2.66	1.43
Subjective norms towards privacy							
SP1	Perception that society expects Internet privacy self-protection	4.55	1.53	4.44	1.54	4.60	1.53
SP2	Privacy protection is an important topic in the social environment	4.36	1.45	4.75	1.55	4.18	1.38
SP3	Fear of social rejection for not being active in social networks	2.77	1.64	2.78	1.77	2.76	1.58
SP4	Fear of social rejection for not sharing pictures in social networks	1.84	1.14	1.78	1.10	1.87	1.17

SD = standard deviation

Items that turned out to have a significant impact on behavior are depicted in **bold**