Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust

YOUNGWOOK DO, Georgia Institute of Technology, USA
JUNG WOOK PARK, Georgia Institute of Technology, USA
YUXI WU, Georgia Institute of Technology, USA
AVINANDAN BASU, Georgia Institute of Technology, USA
DINGTIAN ZHANG, Georgia Institute of Technology, USA
GREGORY D. ABOWD, Northeastern University, USA and Georgia Institute of Technology, USA
SAUVIK DAS, Georgia Institute of Technology, USA

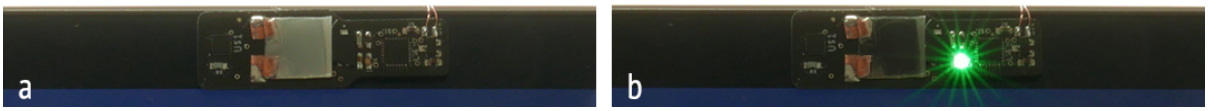

Fig. 1. The Smart Webcam Cover (SWC) automatically covers a webcam when not in use based on the LED indicator status, and requires a manual uncovering when in use: (a) The SWC's PDLC film stays opaque when the LED indicator is off, blocking the webcam view until (b) the LED indicator is on and a user manually presses a button to uncover the webcam.

Laptop webcams can be covertly activated by malware and law enforcement agencies. Consequently, 59% percent of Americans manually cover their webcams to avoid being surveilled. However, manual covers are prone to human error—through a survey with 200 users, we found that 61.5% occasionally forget to re-attach their cover after using their webcam. To address this problem, we developed Smart Webcam Cover (SWC): a thin film that covers the webcam (PDLC-overlay) by default until a user manually uncovers the webcam, and automatically covers the webcam when not in use. Through a two-phased design iteration process, we evaluated SWC with 20 webcam cover users through a remote study with a video prototype of SWC, compared to manual operation, and discussed factors that influence users' trust in the effectiveness of SWC and their perceptions of its utility.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Sound-based input / output**; **Interaction devices**.

Additional Key Words and Phrases: usable security and privacy, privacy-invasive sensor, webcam cover

ACM Reference Format:
Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2018. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/1122445.1122456

Woodstock '18, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Laptop webcams are known points of vulnerability — they can be activated, covertly and without user consent, by malware and allegedly by law enforcement agencies in the U.S. [32, 43]. While it is common for modern laptops to have an associated LED indicator that lights up when the webcam is active, this indicator can be suppressed [9]. Partially owing to this threat — what we call the "covert-spy" attack — one estimate suggests that as many as 59% of U.S. laptop users manually apply a physical cover to their webcams when not in explicit use [7]. Yet, physical covers fully rely on human memory to cover and uncover webcams and are only effective when users remember to use them.

To assess the extent and perceived severity of this problem for end-users, we started with a mixed-methods formative study. First, we ran a survey with 200 webcam cover users in the U.S. and found that 61.5% reported forgetting to cover their webcams at a time when they would have wanted it covered. We next supplemented this survey with a remote interview study with 15 webcam cover users to better understand their motivations for adopting a webcam cover, their reactions to and experiences with forgetting to cover their webcams at a time when they would have wanted it covered, and the strategies they employ to evade webcam surveillance more generally. Most participants reported that the reason they started using a webcam cover was because of their learning about the possibility of covert spying via webcam. Others mentioned the shift to remote work during the COVID-19 pandemic as the immediate catalyst. We found participants' reactions to realizing their webcams were not covered when they wanted them to be could be categorized into two buckets: (i) concern, fear, and embarrassment, and (ii) lack of concern and rationalization. For participants in the former camp, alternative solutions that reduce human error may be particularly pertinent. In other words, while many users feel concerned enough about covert spying attacks to take proactive measures against them, existing solutions solely reliant on human memory can leave users vulnerable, scared, and uneasy.

We introduce a "smart" solution to eliminate the reliance on human memory to cover webcams — Smart Webcam Cover (SWC). SWC automatically covers webcams when the LED indicator associated with their use is off — thereby eliminating the need for people to remember to cover their webcams after they are done using it. While SWC certainly outperforms operation in terms of webcam coverage, our evaluation focused on was on trust and utility. Manual webcam coverage is a reflexive action through which users can convince themselves of their protection, but non-manual solutions eliminate this reflexivity and, in so doing, can reduce users' trust that they are being adequately protected. How can we design SWC to maximize users' trust in its effectiveness? What factors influence perceptions of SWC's utility and practicality? To answer these questions, we employed a two-phased iterative design process.

In the first design iteration, our goal was to model how different design factors might affect users' perceptions of trust and utility in SWC. We implemented SWC in two ways: (i) *PDLC-SWC*: by adjusting the opacity of a Polymer-Dispersed Liquid Crystal (PDLC) film overlaid on top of the webcam; and, (ii) *Motor-SWC*: by mechanically sliding an opaque film to cover or uncover the webcam. We fully automated webcam coverage based on the associated LED indicator state—covering when the LED indicator was on and vice versa. Through a mixed-methods evaluation where we showed participants video prototypes of PDLC-SWC and Motor-SWC, we found that three factors influenced participants' trust in, and their perceived utility of, SWC: (i) the noticeability of a state change from open to closed and vice-versa; (ii) their prioritization of aesthetics; and, (iii) a new adversarial attack against SWC (e.g., a remote control attack in which an attacker who can control the webcam's LED indicator can cover and uncover SWC).

Based on these findings, we created an improved prototype — Hybrid SWC (HSWC) — that (i) builds off the PDLC-SWC form factor to keep its aesthetic advantages; (ii) integrates auditory feedback to alert users to state changes in the cover; and, (iii) requires manual action to uncover the webcam while still automatically covering the webcam when the LED indicator turns off in order to address the emergent remote control attack.

To assess users' trust in and perceptions of the utility of HSWC relative to manual webcam covers, we ran a within-subjects experiment in which we presented participants with two video prototypes of HSWC and the manual webcam cover in counterbalanced order. We had participants rate, on a Likert scale, two statements: (i) to what extent they agreed if HSWC or manual webcam covers would cover the webcam at a time when they would want it closed (timing); (ii) and to what extent they agreed if HSWC or manual webcam covers could cover the webcam completely (opacity). We also asked participants to provide rationales for their ratings.

Our findings suggest that while there is room for improvement in terms of aesthetics and form, participants found HSWC to provide significantly improved protection against covert spying than manual webcam covers and offered sufficient protection against remote control attacks as well. In short, participants trusted the effectiveness of HSWC and found that it had significantly more utility than manual webcam covers.

Concretely, we offer the following contributions in this paper:

- Through a mixed-methods, formative study, we: (i) measured how often webcam cover users forget to cover their webcams at times when they would prefer it to be covered; and, (ii) analyzed the circumstances leading to these episodes of forgetfulness and participants' reactions thereof.
- We followed a two-phased iterative design process to design, implement, and evaluate Smart Webcam Cover — an automated webcam cover that automatically covers laptop webcams when not in clear use in order to thwart covert spy attacks.
- We synthesized implications for the design of smart webcam covers, and other smart physical barriers that protect against intrusive sensing, that inspire trust while reducing reliance on human memory.

2 BACKGROUND AND RELATED WORK

Defending against covert webcam access is a longstanding problem in privacy and security research. We review the causes behind such vulnerabilities and the essential elements for designing SWC in terms of users' control over the data collection and technical solutions for other types of passive data collection technology.

2.1 Covert Webcam Access

Laptops with embedded webcams are often outfitted with a small LED indicator that is meant to alert users when the webcam is in use. However, prior work has demonstrated that webcam indicators can be bypassed altogether, allowing attackers to access users' webcams covertly. For example, there is evidence that law enforcement agencies and malware applications can covertly activate laptop webcams without turning on the LED indicator [43]. Beyond the privileged access granted to law enforcement agencies, Brocker et al. illustrated that the webcam LED indicator embedded in some versions of MacBook laptops can be disabled with only software-based manipulation techniques[9]. With SWC, we help address some of the usability barriers to webcam cover usage by automatically covering and uncovering a webcam based on the LED indicator status. In short, SWC aligns the indication of use with the capability of use.

2.2 User Control Over Passive Data Collection by a Webcam

In addition to laptops, webcams on an increasing number of other smart devices (e.g., smart security cameras) raise privacy concerns of passive data collection without bystander knowledge or consent. Current designs pose technological or intellectual barriers for users to exercise control over such data collection. Specifically, despite claims that smart devices are designed to avoid capturing users' behaviors without their knowledge or consent, there is evidence to the contrary [14, 45]. This suggests that a user's data are susceptible to being passively collected by privacy-intrusive sensors including cameras [9]. Furthermore, while it may be possible to secure access to a user's webcam with only software, webcam users nevertheless believe that their webcam can be accessed without their consent or knowledge [7].

In order to avoid this passive data collection, it is essential that users have control over data collection [42, 49]. Many users attempt to address this vulnerability by installing physical covers that occlude the webcam (e.g., by attaching tape or a sliding barrier) [27, 28, 39]. Machuletz et al. found that these physical barriers can help people feel secure, but that some people stop using a webcam cover for usability (e.g., cumbersome manual operation), aesthetic, and/or social reasons (e.g., not wanting to appear paranoid) [27, 28]. Additionally, passive capture of a webcam could be disabled by disconnecting from the internet [49]. For example, manufacturers have started producing a built-in webcam cover [2, 3] or a kill switch hardwired with webcams[1, 35]. However, such methods rely on human memory to take action, allowing for the possibility that end-users may not perfectly repeat their action [25, 40]. We designed SWC to reduce the risk that users lose their authority for controlling the webcam data collection.

2.3 Technical Solutions against Passive Capture by a Webcam

There are technical solutions to safeguard against passive capture by cameras. Portnoff et al. designed onscreen notifications to better communicate a laptop's webcam activation to users [32]. However, even though such notification techniques may be effective to alert end-users, it does not provide a fail-proof solution [11] and is still subject to manipulation through software control [9]. Other solutions have tried to implement a capture-resistant environment by preventing cameras from recording in an indoor environment. For example, Truong et al. proposed a jamming technique targeting the imaging sensor to prevent undesired video/photo recording [44]. This technique negates the need of a user to manually jam sensing devices but is a coarse approach that produces many false negatives and false positives, reducing its utility in practice. To overcome the existing challenges, our goal for SWC was to develop a fail-safe, intelligent webcam cover that automatically covers the webcam when it is not in use.

2.4 Social Acceptability and Privacy Implications of Cameras

With smartphones, CCTV, drones and IoT home security cameras, cameras are now ubiquitous in both public and private settings, raising concerns of unwitting bystanders being captured without consent [8, 15, 20, 24]. This unwitting capture, in turn, may also introduce social friction between those who use cameras in public settings and the bystanders who may be captured — e.g., if the camera owner captures an embarrassing moment without the bystander's consent [8, 15]. To improve bystander privacy, researchers have studied how to inform bystanders of the status of nearby cameras and protect them from undesirable capture [5, 19, 23, 24]. Most related to the present work, in the field of wearable computing, Koelle et al. argued for the automatic control and physical covering of wearable cameras for privacy-sensitive circumstances, specifically because manual covering is prone to human error [24]. Koelle et al.'s recommendation extends beyond bystander privacy, however — laptop webcam covering is also presently prone to human error, suggesting an automated approach may be appropriate. While bystander privacy is important, it is distinct from our focus in this paper — we focus on protecting individuals from the webcams on their own laptop devices, against threats that can remotely activate these webcams while suppressing the indicators designed to inform users of their use. The constraints, threats and broader design space of a smart webcam cover, thus, differs from automated covers designed to protect bystanders from roving cameras worn or carried by other individuals.

3 THREAT MODEL

Our threat model is an adversary who can remotely, through software, and at any time, access a specific end user's laptop webcam by manipulating the webcam's LED indicator control. The adversary does not have the means to physically manipulate the user's laptop. The goal of this adversary is to monitor or surveil a user through their webcam without their knowledge of consent. This threat model is not theoretical—prior work has

		Objective	Method	Participants Demographic											
				Total	Gender				Age					CS-Edu	CS-Career
					M	F	NB*	UD**	18-24	25-34	35-44	45-54	55-64		
Problem Understanding	Study 1	Measuring Webcam Covering Forgetfulness	Survey	200	93	102	4	1	71	76	32	17	4	47	27
	Study 2	Understanding Webcam Covering Motivation and Concerns about Forgetfulness	Interview	15	6	8	-	-	4	11	-	-	-	13	9
Design Iterations	Study 3	Designing SWC and Understanding Perception of Webcam Cover Users about SWC Design Factors													
	Study 4	Improving and Evaluating SWC Compared to Manual Webcam Covers	Interview Survey	20	9	11	-	-	5	12	2	1	-	13	11

Table 1. The table illustrates our 4-study research framework and demographic information of participants in each study. NB* represents non-binary, and UD** represents participants who did not disclose their gender.

shown that many webcam indicators can be bypassed through malware by law enforcement agencies in the U.S [43]. Our threat model excludes cases where an adversary can access the user's webcam during legitimate use (e.g., while the user is intentionally on a video conference call). These threats will need to be handled differently, since users will know that their webcam is being used but may not be aware of exactly who is privy to their camera feeds.

4 STUDY STRUCTURE

As illustrated in Table 1, we ran four studies. The first two studies were formative assessments to help us understand the magnitude of the problem, of forgetting to cover one's webcam at a time when one would want it covered, from the perspective of the end-user. We started with an an online survey to quantify how many people experienced the problem. We then ran a semi-structured interview study to understand to what extent webcam cover users found these episodes of forgetfulness to be problematic. The final two studies were summative assessments of our interim and final designs of Smart Webcam Cover — part of our broader iterative design approach towards implementing and evaluating Smart Webcam Cover with end-user feedback.

5 STUDY 1: MEASURING FORGETFULNESS IN WEBCAM COVERAGE

Manual webcam covers are only effective against the aforementioned threat model if users remember to use their covers consistently. We hypothesized that many webcam cover users may occasionally forget to cover their webcams at a time they would want it to be covered—memory lapses are a common cause of vulnerability for security systems with humans-in-the-loop [12]. To test this hypothesis and quantify the magnitude of the problem, we conducted an online survey with 200 webcam users across the U.S.

5.1 Method

5.1.1 Recruitment. We used Prolific for recruiting participants and Qualtrics for conducting the survey. We only recruited people who reported using some form of webcam cover on their laptops (e.g., tape, sticky notes, a slide).

5.1.2 Questionnaire. Our questionnaire consisted of 5 questions. First, we asked participants if they could recall a time when they forgot to apply their webcam cover at a time when they would have wanted it closed. As prior work suggests, it is likely that participants would report inaccurate information regarding the frequency with which they forget to close their webcam covers[47]. As such, we instead asked participants to simply recall a concrete, recent instance in which they realized that they had forgotten to cover their webcam at a time when they would have wanted it covered as an interview study described in Section 6. We then asked for demographic information—age, gender, educational background, career types. The full set of questions we asked in our survey is provided in supplementary materials.

5.1.3 Ethics and Compensation. Our study was IRB approved. The survey took users 1 minute to complete on average, for which we compensated participants $0.20 USD ($12/hr).

5.2 Results

In total, 200 webcam cover users completed the survey. We show participant demographics in Table 1. We found that 61.5% of respondents could recall a specific, recent memory in which they forgot to cover their laptop webcam at a time when they would have wanted it to be closed. We found no statistically significant differences across demographic and educational backgrounds. This result suggests that manual webcam covers leave many users vulnerable to covert spying, and there is an opportunity to do better by eliminating reliance on human memory.

6 STUDY 2: UNDERSTANDING USERS' CONCERNS ABOUT WEBCAM COVERING FORGETFULNESS

We next conducted an IRB-approved interview study to dig deeper into participants' reasons for using a manual webcam cover, to better understand the contexts in which they forgot to manually cover their webcams, and to assess to what extent participants found these episodes of forgetfulness to be problematic.

6.1 Method

6.1.1 Recruitment. We recruited 15 participants who reported having an experience with forgetting to cover their laptop webcams at a time when they would have wanted it covered and satisfied our screening criteria. The participants were aged between 18 and 35 years and consisted of 6 males and 9 females. 13 participants had formal education (Bachelor's degree or higher) in computer science, information theory, or a related field (Table 1). We promoted the study on a variety of social media platforms (e.g., Facebook, Slack, Kakao). Before scheduling the interview sessions, we verified participants' eligibility for the study through a set of screening questions.

6.1.2 Procedure. The interviews were conducted over a video conference call to avoid non-essential contact during the pandemic. We asked participants two broad categories of questions: (i) their motivations for starting to use a webcam cover, to better contextualize their experiences of forgetting, as well as to confirm baseline webcam cover usage behaviors found in previous work [27]; and (ii) how they felt after realizing that they had forgotten to manually cover their webcams at a time when they would have wanted it covered.

We initially designed our interview to be 15 minutes long and had planned to provide a 3 USD Amazon gift card as compensation for participants' interview completion. However, due to unanticipated technical challenges (e.g., poor internet connection, poor audio quality), some interview sessions lasted as long as 50 minutes (Mean: 33 minutes, Range: 20-50 minutes). In these cases, we increased compensation retroactively. Thus, with IRB approval, we adjusted our compensation to $10 USD for the average interview time ($12/hr) based on the longest interview time. The full set of questions for the interview is provided in the supplementary materials.

6.1.3 Data Analysis. We performed qualitative coding and thematic analysis on the interview transcripts to identify themes in participants' reactions to forgetting to cover their webcams at an inopportune time. Three members of the research team transcribed the interviews.

One member of the team categorized responses from the transcripts into two buckets, loosely following the structure of the interview itself: (i) why participants used a webcam cover and (ii) their experiences of forgetting to cover. The researcher then performed open coding on each of these categories of responses, iteratively updating the codebook as necessary. A second member of the research team then independently coded the data following

the codebook. The two researchers then together used axial coding to consolidate codes and identify larger themes in the responses.

6.2 Results

From the interview, we identified three motivations for adopting webcam covers. We also found that participants had both emotional and practical reactions to prior experiences in which they had forgotten to cover their webcams at a time when they would have wanted it covered.

6.2.1 Motivations for Webcam Cover Usage. To contextualize their experiences of forgetting to cover their webcams, we first asked participants about their initial motivations for using a webcam cover. We found three such motivations.

Some participants started using a webcam cover after learning about the effects of covert webcam spying through education or media. For example, several mentioned reading anecdotes of being spied upon through the news media. P13 said, "There were some reports online about Facebook, or many websites, having access to your webcam without permissions. So that's when I started putting Post-It notes [on my webcam]." P3 said that seeing the "Shut Up and Dance" episode of British series Black Mirror[1] incentivized them to use a webcam cover; P9 also mentioned this same episode as motivation.

Other participants started using a webcam cover after observing their friends or colleagues using them and felt social pressure to do so as well. For example, P11 stated, "I saw a few of my friends had pieces of tape [on their webcams]...I thought it was pretty sensible." P12 mentioned, "Because I saw other people having the cover on, I got a little self-conscious about it. I was like, 'Wait, maybe I should do that.' " Similar social motivations have been cited for other cybersecurity behaviors in prior work [13].

Another common trigger for using webcam covers was emergent privacy concerns resulting from working from home during the pandemic. Participants noted their colleagues' visibility into their personal home life as a motivating factor: P7, for example, said they started using a webcam cover "when we moved fully online for COVID-19. My workplace and my daily life have merged... My home is where I want to feel comfortable, so that's when I decided to buy one." P12 mentioned that due to working from home, "I'm constantly breastfeeding [my son] throughout the day... My shirt is typically up, or he's on me, and that is not necessarily work appropriate, so I shut [the webcam cover]." However, working from home was often cited in conjunction with the first pattern; the shift of work environments into private spaces due to the pandemic outbreak has thus amplified participants' motivation for using a webcam cover.

Finally, some participants did not make an active decision to use a webcam cover. Rather, their work devices might have had a cover pre-installed (P12), or someone had purchased one for them (P1, P9). Barring work-related shifts due to the pandemic, our findings are largely in line with previously reported motivations for using webcam covers [27].

6.2.2 Emotional reactions: Fear and rationalization. We identified two emergent patterns to participants' emotional reactions when they realized they had forgotten to manually cover their webcams at a time when they would have wanted it covered: (i) concern, fear, and embarrassment and (ii) lack of concern and rationalization.

Concern, fear, and embarrassment. Many interviewees expressed concern that they were potentially vulnerable to covert spying when their webcam was uncovered. Even if their webcam was only uncovered for a brief period of time (i.e., not more than a couple of hours), or if they did not do anything private in the frame of the webcam's view, they were still afraid or embarrassed. For example, P6 shared, "I wasn't doing anything that could be problematic, but still, it's like, it's my personal space and whether I'm doing something peculiar or not,

[1]Black Mirror is a Netflix TV show where each episode illustrates a human-interest story in a technology-fueled dystopia.

regardless of that…it just feels weird." P8, who self-identified as privacy-paranoid, said "I don't trust most of the software, it's opaque to me.…hopefully you know, nobody was watching."

Participants also expressed a fear of the unknown associated with forgetting to cover their webcams. Several participants (P2, P6) noted that while they were fairly confident that nothing malicious had occurred during the uncovering period, the risk that something could have happened was concerning enough. For example, P6, who learned about covert spying attacks and webcam covering practices at both work and school, said, "During the hour, unknowingly, some bad actor could have taken over my camera and done something bad with it." P2, who is pursuing a career in cybersecurity, also said they felt "a little bit embarrassed and a little bit scared because, you know, I don't know what would've happened. Fortunately, my kitchen space is over there, far away, and [the camera] was facing this wall behind me. I didn't do anything weird. So I thought it was fine, but still I was a little bit scared."

Lack of concern and rationalization. In contrast, several interviewees were less concerned with forgetting to cover up their webcam. For example, P1, who started using a webcam cover three weeks prior to the interview since their partner bought it for them, felt that digital protection was already sufficient against covert spying attacks. They mentioned that they did not care much about forgetting to cover their webcam because their "laptop's OS has some kind of tool or program to prevent any kind of hacking…Apple has good privacy protection."

Some participants mentioned that even if they were exposed, they were not worried or concerned about covert spying attacks. They believed that because they were not doing anything private in front of their webcams, it did not matter even if an attacker had spied on them. For example, P10 said, "I did not feel bad, because my laptop is placed in a space where I am always supposed to be professional...they might see me in the kitchen, but nothing sensitive, other than the fact that they would be seeing a stranger." P5 mentioned that their webcam was only open for a short time, so "it wasn't like something drastic going on."

As with past work on the perception of security adoption as paranoia [18], a few other participants said that they did not want to appear paranoid about their webcam cover behavior, since having it closed part of the time already provided some protection. P3, who started using their webcam cover after the pandemic outbreak, said, "If I can cover [the] camera, like, I don't know, eight out of ten times or nine out of ten times, I'm still doing a better job than just having it open all the time. At least I'm making the effort." P7 noted, "I'm not obsessed with it." However, a few participants expressed concern that if an intrusive spying attack had happened to them, then they might have been more alerted and concerned. P3 mused, "Maybe if I did experience some kind of accident, then I would probably have a different mindset... I never had that kind of traumatic events."

Additional findings related to motivation to use webcam covers. We found that participants who started using webcam covers before the pandemic expressed greater concern in response to forgetting to cover their webcams than participants who started using their webcam covers after the start of the pandemic (P1, P3, P4, P7, P9). Additionally, participants who self-identified as privacy-savvy (P2, P6, P8) also demonstrated greater concern.

6.2.3 Practical reactions: Short and long-term mitigating behaviors. Beyond their initial impressions of a lapse in coverage, participants reported engaging in a variety of short and long-term mitigating behaviors to improve their protection against covert spying.

Immediate correction. Unsurprisingly, a majority of participants reported that they closed their covers immediately after noticing it was open. They also supplemented this action with a variety of other techniques to further reduce the possibility of a covert spying attack in that instance. Multiple participants reported closing their laptop lids in order to further ensure that their webcam was blocked off; several also said they closed any applications on their computer that could access the webcam, even if the webcam was not being accessed at that time.

Systemic/long-term behaviors. A few participants who were newer to the webcam coverage practice said that if they got used to closing it, they would eventually remember to do so out of habit. For example, P9 said "Because I'm like a cautious person, . . . if I get used to the webcam cover, then I will never forget this." Other participants reported establishing a habit of glancing at their workspaces where their webcams were located before they left the area, as a cursory check for the state of the webcam cover. Another participant (P5) said that they purchased webcam covers in bulk just in case their covers ever broke, so they would always have a replacement.

Working around the webcam. Finally, some participants accepted occasional lapses in coverage as a reality and adapted their behaviors when knowingly in presence of a webcam. P3 and P4, for example, said that when they saw that the cover was open from across the room, they simply went into a different room to get dressed instead of going over to their laptop to close the cover. Once, for instance, when P4 came out of the bathroom after showering, "It was too much hassle to move all the way to the laptop computer to cover that... I just go right to my bedroom."

7 STUDY 3: FIRST DESIGN ITERATION FOR SMART WEBCAM COVER

Our formative work (Study 1 and 2) suggests that many people are concerned about the covert spy attack, forget to manually close their webcam covers, and consider perceived lapses in coverage to be strongly problematic. Based on these findings, we hypothesized that an automated solution that reduces the need for manual effort in covering one's webcam after it is no longer in use could help solve a common problem that many people find distressing. To that end, we designed Smart Webcam Cover (SWC) to automatically cover or uncover a laptop webcam based on the state of its associated LED indicator: when the indicator is on, the webcam is uncovered; when the indicator is off, the webcam is covered. We settled on this working principle by considering two design factors: (i) fail-safe mechanisms to protect against malfunctions; and (ii) physical-world triggers to protect against covert activation.

7.1 Design Considerations for Smart Webcam Cover

7.1.1 Fail-safe mechanisms to protect against malfunctions. Fail-safe system designs have been widely adapted for scenarios where failing systems are critical to users' safety [10]. A manual webcam cover fails when users forget to cover a webcam. SWC removes failure owing to forgetfulness but may introduce a new failure mode—circuit malfunction (e.g., power loss). Thus, SWC should be designed to be fail-safe: i.e., defaulting to covering the webcam even if it malfunctions.

7.1.2 Physical-world triggers to protect against covert activation. To remove the reliance on human memory in webcam covering, there needs to be a sensible trigger that automatically catalyzes actuation: i.e., covering the webcam when users want it to be covered and vice versa. Our broad goal with SWC was to protect against covert spying attacks where an adversary, through software, can access a user's webcam without activating its associated LED indicator. Since software is unprotected in our threat model, we need a physical-world trigger to ensure alignment between webcam cover state and user's knowledge of webcam activation. A natural trigger for automated actuation, then, is the state of the LED indicator: when the indicator is on, then the webcam should be uncovered (because users can know that it is active and being accessed); when the indicator is off, the webcam should be covered.

7.1.3 Disconnection between a webcam and a webcam cover. One could imagine developing an integrated hardware solution into the laptop itself to protect against the covert spy attack, e.g., a button that could control the angle of the camera lens. However, this integration would directly link the webcam and the protective hardware — a link that could undermine end-user trust, since we assume that users have an implicit distrust of the system that

Fig. 2. This figure demonstrates webcam view difference between with and without PDLC-SWC. Macbook Pro Late 2016 models' FaceTime HD is used for testing: (a) the test distance between a user and a webcam is around 800mm with a sitting position; (b) webcam view without PDLC-SWC; (c) webcam view with PDLC-SWC when the PDLC film turns transparent in a bright environment; (d) webcam view with PDLC-SWC when the PDLC film turns opaque in a bright environment and (e) in a dark environment

operates their webcam if they are concerned about the covert spy attack. To that end, our goal was to develop a disconnected cover, akin to extant manual webcam covers which includes no direct control links between the laptop itself and the webcam cover.

7.2 Smart Webcam Cover Implementation

The SWC we developed consists of two main parts: sensing and actuation. We use a photodetector to sense the state of the LED and actuate the cover in two ways: (i) *PDLC-SWC*: modulating the opacity of a PDLC film, and (ii) *Motor SWC*: sliding a cover onto or off of a webcam using a stepper motor. Although we developed our SWC prototypes based on specifications of Apple's FaceTime HD camera module, our approach should be generally applicable to other laptop webcam modules as well.

7.2.1 PDLC-SWC. PDLC-SWC is designed to cover and uncover a laptop webcam by modulating the opacity of a Polymer-Dispersed Liquid Crystal (PDLC) film overlay. PDLC film technology has attracted attention for smart glass applications due to its unique characteristics, including thin and flexible form factor, easy-to-manufacture material, electrically switchable transmittance, and electrical stability [31].

Sensing. We designed PDLC-SWC based on the dimension and specification of Apple MacBook/MacBook Pro 2015 (or later) models, which lights up a green LED indicator when the webcam is active. To sense the state of the LED indicator, we used a phototransistor (SFH 3410-2/3-Z) that is sensitive to the wavelength of visible green light (See Figure 3 (a) and (b)). To minimize signal interference from ambient light sources (e.g., room lights, laptop backlight), we blocked all the light transmitted around the phototransistor through a light-blocking vinyl electrical tape.

Actuation. For actuation, we took an off-the-shelf PDLC film (HOHO Smart Film) and reshaped it into an 11mm-by-11mm square that can fit in the bezel of a Macbook Pro 2015 [22] (See Figure 3 (c)). This film becomes up to 82% transparent when a voltage between 48 and 65 VAC is applied. (See Figure 2 (d)). Otherwise, the film is opaque, obstructing the webcam view almost completely as shown in Figure 2 (c)). A small fraction of light passing through the opaque film will become highly diffused, greatly reducing the information to the ambient brightness of the room in which the laptop is situated (See Figure 2 (d) and (e)). As the phototransistor in PDLC-SWC blocks the green light of the MacBook webcam LED indicator, we embedded an extra LED on the PCB for users to be able to see the LED indicator.

PCB Design and Fabrication. The MacBook models we targeted have a narrow clearance between the display and keyboard. Thus, any device thicker than 1.5mm could damage the display [21]. Therefore, a key design challenge was to keep the thickness of PDLC-SWC to 1.5mm or less while integrating all the essential components around the webcam in the bezel of the display. To address this challenge, we created a cavity to fit the phototransistor with a height of 1.05 mm, such that it can be placed facing the laptop LED indicator

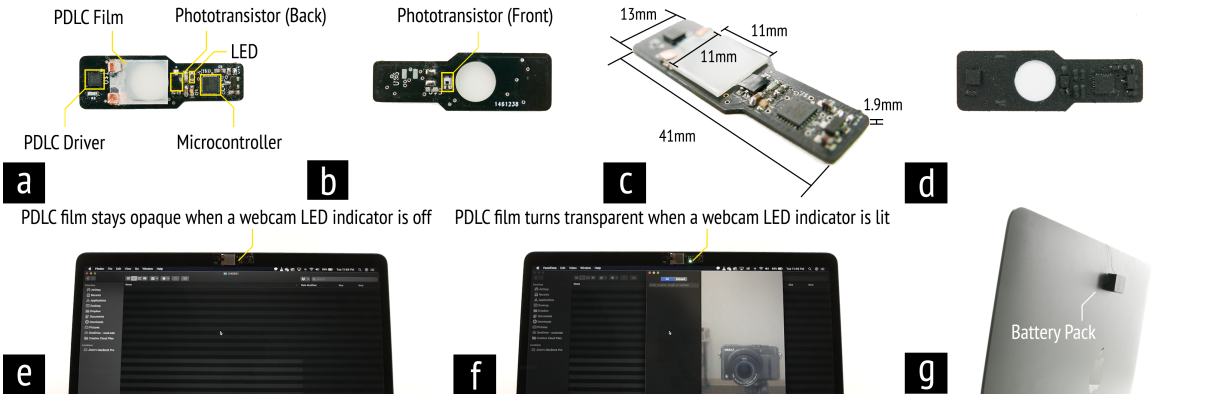

Fig. 3. We develop PDLC-SWC; This figure illustrates (a) front-side view; (b) backside view; and (c) the dimension of the PDLC-SWC. (d) PDLC-SWC can be coated with the LTS-400 coating spray to make the look unobtrusive from the laptop bezel when it is installed. PDLC-SWC is installed by aligning the phototransistor to a laptop's LED indicator. The PDLC transmittance changes (e) cover and (f) uncover the webcam by sensing the LED indicator's activation status. In this example, we opened Apple's FaceTime application to activate a webcam and its LED indicator. (g) The current PDLC-SWC uses a 3.7V 60mAh Li-po battery for the actuation power source.

and connected on the other side. Note that the overall height of PDLC-SWC is higher than 1.5mm due to the low-dropout regulator (AP2138N) as shown in Figure 3 (c). Since it could be relocated from the mainboard to the battery pack, PDLC-SWC's form factor could be improved to fit the clearance of MacBooks. We made a hole in the middle of the PCB for the webcam to see through. The relative positioning of the hole to the phototransistor helps ensure that the phototransistor is aligned on top of the laptop LED indicator (See Figure 3 (a) and (b)). Due to the thickness tolerance of the design, we attached the battery to the laptop cover and connected it with thin magnet wires (See Figure 3 (g)). To manage the sensing and actuation parts, we used an ultra low-power micro-controller (STM8L151G4U6TR) to save power and an electro-luminescent lamp driver (HV853K7-G) to drive high voltage for PDLC activation. (See Figure 3 (a))

Power Consumption and Form Factor. The power consumption is 76.6mW when the device is operating, and the PDLC film is transparent, and 1.49mW in the standby state. If a user uses the webcam for 2.5 hours a day, PDLC-SWC with the 60mAh battery can use one day on a single charge. To minimize malfunctions and damage that could result from touching the surface of the PCB, we coated the PCB with a rubberized electrical insulation spray (LTS-400 by Gardner Bender), and the battery attached to the laptop cover was protected with a 3D-printed secure case.

Fail-Safe. If the battery that powers the PDLC film runs out, the PDLC will remain opaque. In this way, the PDLC film provides safety by default. Note that there are other ways in which SWC could fail that would not necessarily guarantee safety — e.g., if the phototransistor we use to detect the state of the MacBook LED indicator accidentally detects the LED as being active when it is not. In practice, these situations can be avoided by providing adequate instructions for users to install and secure the SWC properly.

7.2.2 Motor-SWC. Motor-SWC is designed to obscure the webcam by sliding a cover back and forth with a tiny stepper motor. Most parts of Motor-SWC are the same as that of PDLC-SWC — only the actuation mechanism is different.

Sensing. We use the same implementation as PDLC-SWC's sensing module.

Actuation. Motor-SWC automatically slides a cover over or off of a webcam. We implemented Motor-SWC with a stepper motor and a linear screw slider block. When the phototransistor detects light from the webcam

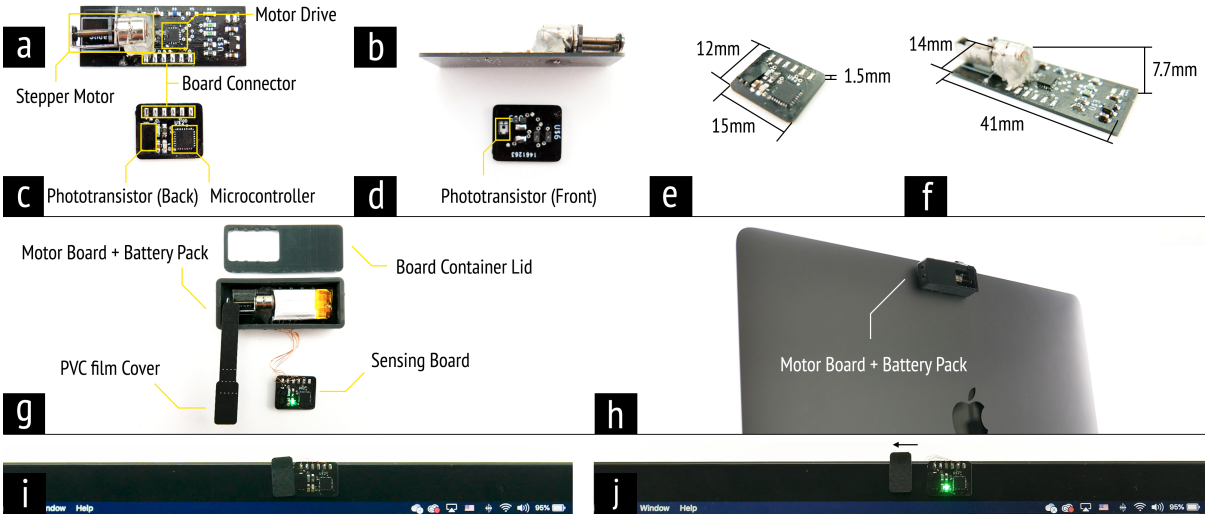

Fig. 4. Motor-SWC consists of a motor drive board ((a) front view; (b) side view) and a sensing board ((c) front view; (d) side view); (e) The sensing board dimension; (f) The motor drive board dimension; (g) Full-integration of the sensing board, the motor drive board, and its battery pack; (h) The motor drive board and the battery pack are installed on a laptop's lid; (i) the PVC film cover connected with the motor blocks a webcam when a webcam LED indicator is off; (j) Otherwise, the PVC film slides to uncover the webcam.

LED indicator, it opens the slider. Otherwise, it blocks the webcam by closing the slider. Unlike PDLC-SWC, it only uses power when changing between the open and closed states. In addition, Motor-SWC produces an auditory cue when it changes state, which can help make its functionality more apparent relative to PDLC-SWC.

PCB Design and Fabrication. Due to the height of the stepper motor, we could not put it on the display bezel around the webcam. Thus, we divided the PCB board into two parts—sensing and actuation and attached the actuation part to the back of the laptop screen together with the battery. These two parts are connected through thin magnet wires. We used the same micro-controller (STM8L151G4U6TR) for sensing and actuation as the PDLC-SWC's modules and a low voltage stepper motor driver (STSPIN220) to control the motor (See Figure 4).

Power Consumption and Form Factor. The power consumption of Motor-SWC is 315.5mW when the stepper motor changes its state (e.g., from open to closed or vice versa), 11.1mW while the green LED is on, and 6.6mW in the standby state. If a user uses the webcam for 2.5 hours a day, Motor-SWC with the 60mAh battery can be used for 1.1 days on a single charge. Similar to PDLC-SWC, the sensing part of Motor-SWC was coated with the rubberized electrical insulation spray, and the actuation part and battery attached to the laptop cover was protected in a single 3D-printed secure case (See Figure 4).

Fail-Safe. Unlike PDLC-SWC, Motor-SWC is not fail-safe against battery depletion: the motor will be stuck once its power source runs out. We can partially guard against this by preventing the cover from opening if the battery level is too low.

7.2.3 Usability Challenges. Unlike a manual webcam cover, SWC requires a power source to enable automatic covering and uncovering continuously. As both PDLC-SWC and Motor-SWC use a battery that has the limited amount of charge, they will need to be recharged occasionally. The need to recharge is likely to reduce the usability of the device since users may forget to recharge devices. Additionally, as SWC requires a battery pack to operate, SWC would be bulkier than manual webcam covers, which could limit the SWC's usability. In the Discussion section, we suggest future designs that can help address some of these concerns. Finally, as SWC

operates based on a webcam's LED indicator, SWC only works on laptops with an associated webcam LED indicator.

7.3 Evaluation

SWC can better protect against the covert-spy attack via laptop webcams than manual webcam covers. However, as opposed to manual webcam coverage, SWC eliminates the reflexive covering action through which users can convince themselves of their protection. Will users trust an automated solution? Which form-factor of SWC will elicit greater trust? Which form-factor might users prefer?

To evaluate SWC and answer these questions, at the end of the interview study conducted in Section 6, we presented participants with video prototypes of both PDLC-SWC and Motor-SWC in counterbalanced order [2]. We asked participants about their preferences among and trust in the two prototypes versus a manual webcam cover, and why. We used the first version of our working prototypes in creating the video prototypes, following the study we made additional improvements. Before starting the interview, we had a Q&A session to answer participant questions. The full set of questions we asked for the interview are provided in the supplementary materials. We used the same qualitative coding methodology described in Section 6.1.3 to analyze the data.

We found three major factors influenced participants' perceptions and preferences between our prototypes: trust, form, and new adversarial attacks against Smart Webcam Cover. In short, we found that while participants trusted more in the functionality of Motor-SWC, they found its form impractical. In contrast, while participants expressed skepticism about the effectiveness of PDLC-SWC, they appreciated its sleeker design.

7.3.1 Trust in the functionality of SWC. Participants' trust in SWC centered primarily around its actuation mechanism rather than the automation itself. Participants trusted in SWC's ability to detect the LED indicator, but felt more confident in the effectiveness of Motor-SWC than PDLC-SWC. Three factors played into this preference: noticeability, familiarity, and vulnerability.

Noticeability. Many participants felt that both the familiar horizontal covering motion of Motor-SWC and the whirr of its stepper motor provided noticeable visual and audio cues that the cover was working. P4 said that the motion "lets me know that it's doing its job of covering and opening the camera." P6 said, "If I see hardware that's actually going over the camera...I know that this actually closed." P9 noted, "There's a motor sound, zeekzeek! ... So it will help me realize that now it is covering the cam, or now it is opening the camera." P4 also mentioned Motor-SWC's unintended accessibility features: "It has a sound [from the motor] so [visually impaired] people can be alerted."

On the other hand, participants found the state-change of the PDLC-SWC harder to notice. P12 wondered, "Would it be visible for me to see that it's opaque [or] transparent if I wasn't looking at a video...like if I was just looking at the camera and had not turned on Zoom? Is it very obvious that it's opaque? How would I know that it was working?"

Familiarity. Many participants liked that Motor-SWC felt similar to the covering action for manual webcam covers: P6 noted, "It more closely mimics what the human user would do — it's just doing the sliding back and forth for us basically," and P8 said, "It functions the same way like the cover that I have right now, and it is automatic." Generally, participants felt confident that because Motor-SWC involved a solid piece of material moving horizontally, it was adequately covering the webcam.

On the other hand, most participants were unfamiliar with PDLC films and expressed skepticism about whether it would fully protect them. P5 said they wanted approval from the people around them that the PDLC material was safe to use. Others' skepticism was rooted in unfamiliarity about how PDLC worked. The fail-safe mechanism of the PDLC-SWC did not necessarily assuage these concerns. P2, who was familiar with the material beforehand, expressed some discomfort and doubt: "I've seen [in Japan] public restrooms that use this technology...I still have

[2]We included the PDLC-SWC and Motor-SWC video prototypes in supplementary materials

some sense of disbelief. What happens if this malfunctions? Even if it says it has a fail-safe mechanism, this is like psychology."

Vulnerability. Finally, several participants also said that the protection of PDLC-SWC was not absolute, and that the potential for light-leakage concerned them. For example, P2 remarked, "Maybe the hacker is interested in whether you are at home or not...you can still get a glimpse of whether [your room] is dark or whether you're in a lit situation."

7.3.2 Form informs preference. The second factor that affected participants perceptions of our SWC prototypes was form—specifically, bulkiness and durability. Whereas participants tended to trust more in the familiar functionality of Motor-SWC, they preferred the look of PDLC-SWC.

Bulkiness. Participants overwhelmingly felt that Motor-SWC was too bulky. Many remarked that they were worried they could not close their laptops fully if Motor-SWC was attached, as the thickness of the cover would leave a gap from the laptop lid. Participants also wondered if Motor-SWC might damage their computer if it was sandwiched in that gap; one participant mentioned previously switching from a manual sliding cover to sticky notes to cover their webcam because the gap caused by the sliding cover had caused damage to their device. P6 said, "Even if I got the motor one for free, I don't think I'd use it unless it got smaller and silent." P10 worried about the social acceptability of Motor-SWC [13, 33], stating "I don't want to look like a freak when I am going in public with a motor [stuck onto my laptop]." In contrast, participants liked the thinner form factor of PDLC-SWC. Several said that it was sleeker; one participant believed it would be more adaptable to more laptops.

Durability. Participants felt that Motor-SWC was more fragile due to its bulk and because it protruded from the top of the laptop. They worried not only that Motor-SWC would damage their own devices, but also that they would accidentally damage Motor-SWC through daily use: e.g., putting the laptop into a sleeve or backpack (P12), accidentally sitting on the laptop (P5), or simply closing the laptop lid with too much force (P7). In terms of durability, participants felt that there was less to worry about with PDLC-SWC overall, but P9 still expressed concern about the PDLC material itself: "If there's some defect on the film, then maybe they can see some of our faces or some of us through that webcam. [The quality of the film] could drop."

7.3.3 The remote control attack: an emergent attack against Smart Webcam Cover. Lastly, while automated control eliminates the reliance on human memory for webcam covering, P10 expressed concern about a new type of attack enabled by SWC: adversaries who can control the webcam LED indicator could, in turn, control SWC. For example, by switching on the LED indicator, an adversary could open the cover without the user's consent — even if the user knows that the adversary is doing so. We call this new threat the "remote control" adversary.

8 STUDY 4: SECOND DESIGN ITERATION FOR SMART WEBCAM COVER

From Study 3, we found that while the noticeability and familiarity of Motor-SWC's actuation mechanism helped participants trust its efficacy, participants preferred the sleeker form-factor of PDLC-SWC for practical use. Additionally, such automated solutions could be vulnerable to the "remote control" attack. Combining these findings, we implemented a new iteration of Smart Webcam Cover — Hybrid SWC (HSWC).

8.1 Smart Webcam Cover Design Improvement based on First Design Iteration

Based on our findings from the previous study, we based our design of HSWC on the following considerations:

8.1.1 Thin Form Factor for Preference. Participants in the previous study preferred PDLC-SWC because it was thinner and less obtrusive. Therefore, we used PDLC-SWC as the base for HSWC.

8.1.2 Auditory Feedback for Trust. Participants in our previous study valued the auditory feedback that Motor-based SWC provided in changing state from open to closed and vice versa. Specifically, becoming aware of state

Fig. 5. This figure shows how HSWC works: (a1) HSWC is attached same as PDLC-SWC; (a2) The button and buzzer are contained in a container and are attached on the laptop lid; (b1) Even if a webcam is activated, the PDLC film stays opaque and the LED indicator is blinking, which indicates that the cover is closed; (b2,b3) A user needs to press the button manually to unblock the webcam

changes can help build trust that the automated cover is working as expected. For HSWC, we integrated a tiny buzzer (Mallory Sonalert's AST0540MW) to provide auditory feedback to indicate that the cover has changed state (see Figure 5 (a2)). The buzzer produces an ascending or descending tone to indicate covering and uncovering, respectively.

8.1.3 Automatic Covering, Manual Uncovering. To address the remote control attack, we outfitted HSWC with a small, manual button that must be pressed to uncover the webcam. Covering, however, remains automatic and tethered to the state of the LED indicator. Thus, HSWC requires explicit user action to uncover, but still automatically covers the webcam when the webcam is not in use — addressing both the remote control and covert spy attacks (See Figure 5 (b)). Moreover, this approach adheres to design suggestions from prior work on employing shutter mechanisms for camera-based devices to make privacy more tangible [4]. The button was integrated into the battery pack for HSWC (See Figure 5 (a2)).

8.2 Evaluation

HSWC protects against the covert spy and remote control attacks, but how do users weigh the importance of this protection versus the added complexity? How might users trust in the effectiveness of HSWC compared to a manual webcam cover? To answer those questions, we ran a second remote, mixed-methods evaluation of SWC with both participants from the previous study as well a new set of participants.

8.2.1 Recruitment. With the same participation eligibility criteria as the previous study, we recruited 20 participants who reported having forgotten to cover their laptop webcams when they wanted them to be covered (Table 1). Specifically, we recruited 10 participants who participated in the previous study (Study 3) and 10 new participants. We recruited participants via: (i) follow-up emails to the participants who participated in the previous study, (ii) our institutional mailing list, and (iii) social media.

8.2.2 Procedure. We ran a 30-minute remote evaluation and provided a 6USD Amazon gift card as compensation. The sessions were conducted over the BlueJeans video conferencing tool. Our primary goal was to assess how participants viewed Hybrid-SWC relative to manual webcam covers in terms of coverage effectiveness, which we broke down into timing (i.e., the webcam is covered when it should be covered and uncovered when it should be uncovered) and opacity (i.e., when covered, the cover completely occludes the webcam).

Our evaluation was a counter-balanced, within-subjects experiment with two conditions: Hybrid-SWC and manual. Participants were shown a video prototype for both Hybrid-SWC and a manual webcam cover in

counter-balanced order [3]. Following their viewing of each video prototype, we asked participants to rate, on a 5-point Likert-scale ranging from Strongly Disagree to Strongly Agree, their agreement with the following two statements:

- *Timing*: The Smart Webcam Cover/Manual Webcam Cover always cover my webcam when I want it closed.
- *Opacity*: The Smart Webcam Cover/Manual Webcam Cover will cover my webcam completely.

We also asked participants for the rationale behind their ratings, and any other general impressions they had towards the prototype. [4]

8.2.3 Data Analysis. We performed qualitative coding and thematic analysis on the interview transcripts to identify emergent themes in participants' reactions to both HSWC and the manual webcam cover. For the Likert-scale questions on coverage timing and opacity, we tallied the number of participants that rated HSWC higher than the manual webcam cover.

8.3 Results

8.3.1 Qualitative Findings. Participants re-iterated a number of comments that we found from our initial evaluation in Study 3 (e.g., the familiarity of the PDLC film, the durability of SWC components) (See section 7.3). Beyond these reiterations, however, we also identified three new themes: False Perception about HSWC's Manual Uncovering for Agency; Practicality; and Reactions around Webcam Cover Design.

False Perception about HSWC's Manual Uncovering for Agency. Several participants expressed feeling safe and assured against the covert spy and remote control attacks afforded by automatic covering and manual uncovering. P19 said "I think that's a pretty intuitive approach. It's a on-demand kind of style, where you're only allowing the computer to use their software... and when you do not intend to use it, then it shuts off... It also gets rid of the need to always, you know, remember to cover the camera.".

Some participants questioned the need for manual uncovering because of the expectation that "Smart" devices should be automatically controlled. For example, P11 mentioned "I think, obviously, like automatic [uncovering] would be, would be cool. And it would be useful..." Some of these participants later realized the need for manual uncovering by reflecting on the potential for a remote control attack without manual uncovering. Indeed, P11 later mentioned "But, I also like the idea that you're the one that's uncovering your camera... you want to be in control of the one uncovering it." P15 added "What if someone who's spying on you overrides the LED and then turns on the camera without the LED... nah... It's still going to be opaque... I think that's the only way you could perfectly prevent those spying attacks from happening."

Practicality. Participants also discussed the practicality of using HSWC. First, some found the button position — on the laptop lid — inconvenient. P7 mentioned "Pressing a button on the back seems really finicky... That kind of seems very inaccessible." P12 said "one thing I would dislike is purely... is that the button is very far away from the actual webcam." To that end, they suggested placing the button on the webcam side so that they can press the button as if they use the manual webcam cover.

In addition, participants asked about the durability of PDLC film–how many switching times it can endure in order to set the expectation about the value of HSWC. Several participants mentioned that they expected the film to endure longer than a manual webcam cover. P3 said "I'm probably going to replace this post-it note in probably like, a couple month... if the smart webcam cover's lifespan of like, three, four years, then I'm very satisfied with that." Additionally, participants revealed economic preferences for the HWSC. P12 said "I'd probably be willing to pay like... maybe 5 to 7 USD... it's like one of those risk mitigation type things."

[3] We included the HSWC and manual webcam cover video prototypes in supplementary materials
[4] We included our full questionnaire in the supplementary materials.

Reactions around Webcam Cover Design. Unsurprisingly, aesthetics and design were important considerations. P15 mentioned "I personally find [HSWC] ugly... I could see the board and some wire." Other participants felt the opposite — P3 and P9 mentioned the word 'cool' about SWC's functionality and looks.

Manual webcam covers were also met with similarly ambivalent reactions. P7, who self-identified as a designer, disliked the idea of placing something that was not blended into the laptop bezel on a webcam. However, P11 and P19 argued that they want the webcam cover to stand out from the laptop bezel to remind them to cover their webcam.

8.3.2 Quantitative Results. For the coverage time question, 15 participants rated HSWC higher while three participants rated HSWC lower than the manual webcam cover. On the other hand, for the coverage opacity question, 8 participants rated HSWC higher while 6 participants rated HSWC lower than the manual webcam cover.

Specifically, for *Timing*, the medians of manual webcam cover and HSWC were 3 and 5, respectively. A Wilcoxon Signed-rank test showed that participants were significantly more likely to agree that HSWC would keep their webcams covered when they would it covered than a manual webcam cover ($W = 25$, $Z = -2.73$, $p < 0.01$, $r = 0.61$). For *Opacity*, we did not find evidence to suggest that participants found HSWC to be more effective than a manual webcam cover —the medians of manual webcam cover and HSWC were 4 and 4, respectively ($W = 33.5$, $Z = -0.60$, $p > 0.5$, $r = 0.13$).

In short, our findings from the questionnaire and the interview suggest that while there is room for improvement in terms of aesthetics and form, participants found HSWC to provide better coverage and protection against covert spying than manual webcam covers, and provided sufficient protection against remote control attacks as well.

9 DISCUSSION

Beyond the immediate insights gleaned from our user evaluations, we next discuss design implications, limitations, future work, and the potential for our work to open up broader design space for smart physical barriers that protect against privacy-intrusive sensors.

9.1 Deployability

For most people, cybersecurity is a secondary concern [16, 26, 29]. Thus, people who are only somewhat concerned about covert spying through their laptop webcam are unlikely to purchase an expensive, bulky, or power-consuming apparatus to address that threat. Exploring practical deployability, while out of scope for our present contribution, is nevertheless an important consideration for future work.

9.1.1 Cost. The cost to produce SWC will likely be higher than the cheapest manual solution (i.e., a piece of tape) even if the manufacturing costs of SWC were optimized and produced at scale. Future work may focus on measuring the price that people would be willing to pay for SWC, to see if it would be economically viable for mass production.

9.1.2 Power. Currently, all the SWC prototypes can last for a full day without a recharge. The need to recharge the webcam cover reduces its usability [38]. There are four ways we envision this challenge can be addressed, each with trade-offs. First, we can use a larger capacity battery. Since there are thin and wide batteries on the market, we can develop a battery pack that looks like a decorative sticker. Second, SWC could be connected to the laptop to keep it charged. This would ensure a stable power source, but has a key weakness: if there is a direct link between the laptop and SWC, attackers may be able to access SWC through the laptop and find creative ways to compromise its functionality. Third, SWC could be self-powered by embedding, e.g., a solar panel that harvests ambient energy. This could increase the bulkiness of the design, however. Fourth, assuming it is cheap

enough, SWC could be shipped with a limited operational lifespan and be replaced as needed. Many consumer electronic products already operate under this model. This option would be more wasteful, however, and would require users to swap out SWC modules regularly.

9.1.3 Form Factor. Manual webcam covers are small and thin. SWC, while thin enough to remain affixed to the laptop screen when it is closed, invariably has a larger footprint since it needs a battery and a microcontroller to function. Minimizing bulk and improving aesthetic appeal will be critical to ensuring practical deployability.

9.1.4 LED Indicator Status Sensing. SWC relies on the laptop's associated LED indicator status to determine when the webcam should be covered. This approach comes with challenges.

First, if SWC is not accurately placed on one's laptop, its functionality could be hindered. Specifically, if SWC's phototransistor is misaligned with the webcam LED indicator, it might sense light sources (e.g., ambient light) other than the webcam LED indicator and incorrectly cover the webcam when it should be uncovered. Importantly, it would still require users to manually uncover their webcam in the event that it inaccurately senses that the LED indicator is on when it is not. In practice, it should be possible to avoid this problem by providing end-users with clear installation instructions.

Second, SWC is not suitable for devices that have no webcam LED indicator. We did not consider these devices because they are not material to our covert spy threat model — indeed, with no webcam LED indicator, a remote attacker has nothing to suppress to give users a false sense that they are not being watched. Still, it would be pertinent to explore other types of signals that could inform users as to the activation status of their webcams; these signals, in turn, could then be used as alternative triggers for SWC.

9.1.5 Potential Design and Material for Smart Webcam Cover. Laptop manufacturers recommend for users not to use a webcam cover as they can damage laptop screens [6] and occlude other sensors, such as the ambient light sensor used to operate a monitor display brightness automatic control [34]. These issues could be resolved with a webcam cover structure that does not block the ambient light sensor, and soft material-based actuators to avoid damaging the display (e.g., paper-based [46], silicone-based [17, 30, 48] actuators).

9.2 Ecological Validity and Future Directions

Our evaluations were limited to remote video prototypes, partially owing to the COVID-19 pandemic. Additionally, participants in our studies were not necessarily representative of a general population of laptop users — indeed, over half of our participants reported having a background or education in computer science. Also, our sample was limited to the U.S. population. In the future, it would be pertinent to run a long-term "in-the-wild" study for SWC with a more diverse, representative population of participants.

In addition, prior work in security warning design suggests that users get *habituated* to and learn to ignore cues after repeated exposures [36, 37, 41]. In a longer-term field deployment, would participants continue to notice the covering and uncovering of SWC, or will they get habituated to it and ignore these cues? How might habituation affect their trust in SWC? In future work, we look forward to tackling these questions through a broader field study.

9.3 Design Opportunities for Smart Physical Barriers against Privacy-intrusive Sensors

As people are increasingly surrounded by privacy-intrusive sensors (e.g., cameras, microphones) in their everyday physical environments, there is an opportunity to explore the design space of intelligent physical barriers to protect against these sensors. SWC is an instantiation of a broader class of physical privacy barriers that align sensor usage with knowledge of its usage. Extended from a physical barrier for a webcam, it would be interesting to examine if the key design elements of SWC can be applied to designing an intelligent physical barrier for other types of sensors.

As an example, one potential direction is a physical barrier for smart speakers. As their microphones are designed to be activated by trigger words (e.g., "Hey Siri"), it is unclear to users if the microphones are listening to their private conversations as well. A compelling direction for future work might be to identify how to implement physical privacy protections to ensure that a microphone can hear a user's voice only when it is obvious that it is listening.

10 CONCLUSION

Laptop webcams can be covertly activated, leaving users at risk of surreptitious surveillance by malicious actors and law enforcement. Owing to this threat, many users report using manual webcam covers to obstruct their webcams when not in use. But manual webcam covers rely on human memory and are prone to human error. Indeed, in a survey with 200 webcam cover users in the U.S., we found that 61.5% reported forgetting to cover their webcams at a time when they would have wanted it covered and that many had strong emotional reactions to these lapses in coverage. We employed a two-phased iterative design process to design, implement and evaluate SWC — a webcam cover that automatically covers laptop webcams to thwart the covert spy attack without relying on human memory. We found evidence to suggest that participants found the final iteration of SWC — HSWC — to be significantly more effective than manual webcam covers at protecting against covert spying attacks while also providing protection against a new class of attack that might be introduced using automated solutions — the remote control attack. More broadly, our work is an illustrative example of a new class of smart physical privacy barriers that protect against intrusive sensing in the physical world while removing or reducing reliance on human memory.

REFERENCES

[1] 2014. Purism Librem 14. https://puri.sm/ (Accessed on 09/07/2020).

[2] 2018. Facebook Portal. https://portal.facebook.com/. (Accessed on 09/07/2020).

[3] 2020. ThinkPad X1 Extreme Gen 2 Laptop. https://www.lenovo.com/us/en/laptops/thinkpad/thinkpad-x1/X1-Extreme-Gen-2/p/22TP2TXX1E2 (Accessed on 09/07/2020).

[4] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[5] Rawan Alharbi, Mariam Tolba, Lucia C Petito, Josiah Hester, and Nabil Alshurafa. 2019. To mask or not to mask? balancing privacy with visual confirmation utility in activity-oriented wearable cameras. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies* 3, 3 (2019), 1–29.

[6] Apple. 2020. Don't close your MacBook, MacBook Air, or MacBook Pro with a cover over the camera. https://support.apple.com/en-us/HT211148

[7] Jenni Balthrop. 2019. HP Survey highlights webcam security and privacy behaviors. https://press.hp.com/us/en/press-releases/2019/awareness-of-webcam-hacking.html. (Accessed on 09/09/2020).

[8] Andrew Besmer and Heather Richter Lipford. 2008. Privacy perceptions of photo sharing in facebook. In *Proc. SOUPS*, Vol. 8.

[9] Matthew Brocker and Stephen Checkoway. 2014. iSeeYou: Disabling the MacBook Webcam Indicator {LED}. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. 337–352.

[10] Richard B Chase and Douglas M Stewart. 1994. Make your service fail-safe. *MIT Sloan Management Review* 35, 3 (1994), 35.

[11] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[12] Lorrie F Cranor. 2008. A framework for reasoning about the human in the loop. (2008).

[13] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 143–157.

[14] Matt Day, Giles Turner, and Natalia Drozdiak. 2019. Is Anyone Listening to You on Alexa? A Global Team Reviews Audio. https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio

[15] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2377–2386.

[16] Paul Dourish, E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[17] Jack Forman, Taylor Tabb, Youngwook Do, Meng-Han Yeh, Adrian Galvin, and Lining Yao. 2019. ModiFiber: Two-Way Morphing Soft Thread Actuators for Tangible Interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–11.

[18] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. 2006. Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 591–600.

[19] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 571–582.

[20] Giovanni Iachello, Khai N Truong, Gregory D Abowd, Gillian R Hayes, and Molly Stevens. 2006. Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 1009–1018.

[21] Apple Inc. 2020. Don't close your MacBook, MacBook Air, or MacBook Pro with a cover over the camera. https://support.apple.com/en-us/HT211148 (Accessed on 09/12/2020).

[22] Shanghai HOHO Industry. [n.d.]. HoHo Smart PDLC Film. http://www.hohotint.com/list-10-1.html (Accessed on 09/12/2020).

[23] Marion Koelle, Torben Wallbaum, Wilko Heuten, and Susanne Boll. 2019. Evaluating a Wearable Camera's Social Acceptability In-the-Wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.

[24] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED status lights-design requirements of privacy notices for body-worn cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction*. 177–187.

[25] Phillippa Lally, Cornelia HM Van Jaarsveld, Henry WW Potts, and Jane Wardle. 2010. How are habits formed: Modelling habit formation in the real world. *European journal of social psychology* 40, 6 (2010), 998–1009.

[26] B. W. Lampson. 2004. Computer security in the real world. *Computer* 37, 6 (June 2004), 37–46. https://doi.org/10.1109/MC.2004.17

[27] Dominique Machuletz, Stefan Laube, and Rainer Böhme. 2018. Webcam covering as planned behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[28] 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*.

[29] Tyler Moore. 2010. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection* 3, 3 (2010), 103 – 117. https://doi.org/10.1016/j.ijcip.2010.10.002

[30] Ryosuke Nakayama, Ryo Suzuki, Satoshi Nakamaru, Ryuma Niiyama, Yoshihiro Kawahara, and Yasuaki Kakehi. 2019. MorphIO: Entirely Soft Sensing and Actuation Modules for Programming Shape Changes through Tangible Interaction. In *Proceedings of the 2019 on Designing Interactive Systems Conference*. 975–986.

[31] Sucheol Park and Jin Who Hong. 2009. Polymer dispersed liquid crystal film for variable-transparency glazing. *Thin Solid Films* 517, 10 (2009), 3183–3186.

[32] 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 33rd Annual ACM Conference on Human Factors in Computing Systems*. 1649–1658.

[33] Halley P Profita, James Clawson, Scott Gilliland, Clint Zeagler, Thad Starner, Jim Budd, and Ellen Yi-Luen Do. 2013. Don't mind me touching my wrist: a case study of interacting with on-body technology in public. In *Proceedings of the 2013 International Symposium on Wearable Computers*. 89–96.

[34] Sam Rutherford. 2020. Apple Warns Against Closing Your Laptop While Using a Webcam Cover. https://www.gizmodo.co.uk/2020/07/apple-warns-against-closing-your-laptop-while-using-a-webcam-cover/ (Accessed on 09/08/2020).

[35] Marc Saltzman. 2020. Webcams are infiltrating your home. Here's how to secure those on your computers. https://www.usatoday.com/story/tech/columnist/2020/02/15/webcam-security-heres-some-simple-tips-protect-your-privacy/4749529002/

[36] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The emperor's new security indicators. In *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 51–65.

[37] David Sharek, Cameron Swofford, and Michael Wogalter. 2008. Failure to recognize fake internet popup warning messages. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 52. SAGE Publications Sage CA: Los Angeles, CA, 557–560.

[38] Thad Starner. 2001. The challenges of wearable computing: Part 1. *Ieee Micro* 21, 4 (2001), 44–52.

[39] Thad Starner. 2001. The challenges of wearable computing: Part 2. *Ieee Micro* 21, 4 (2001), 54–67.

[40] Katarzyna Stawarz, Anna L Cox, and Ann Blandford. 2015. Beyond self-tracking and reminders: designing smartphone apps that support habit formation. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2653–2662.

[41] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness.. In *USENIX security symposium*. Montreal, Canada, 399–416.

[42] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[43] Craig Timberg and Ellen Nakashima. 2013. FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance. *The Washington Post* (Dec 2013). https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html

[44] Khai N Truong, Shwetak N Patel, Jay W Summet, and Gregory D Abowd. 2005. Preventing camera recording by designing a capture-resistant environment. In *International conference on ubiquitous computing*. Springer, 73–86.

[45] Kurt Wagner. 2020. Facebook Shared User Data With Developers Longer Than Promised. https://www.bloomberg.com/news/articles/2020-07-01/facebook-shared-user-data-with-developers-longer-than-promised

[46] Guanyun Wang, Tingyu Cheng, Youngwook Do, Humphrey Yang, Ye Tao, Jianzhe Gu, Byoungkwon An, and Lining Yao. 2018. Printed paper actuator: A low-cost reversible actuation and sensing method for shape changing interfaces. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[47] Huiying Yan. 2020. *Memory Bookmarking: Using In Situ Information to Promote Recall in Online Data Collection.* Ph.D. Dissertation.

[48] Lining Yao, Ryuma Niiyama, Jifei Ou, Sean Follmer, Clark Della Silva, and Hiroshi Ishii. 2013. PneUI: pneumatically actuated soft composite materials for shape changing interfaces. In *Proceedings of the 26th annual ACM symposium on User interface software and Technology*. 13–22.

[49] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.