Somebody's Watching Me?

Assessing the Effectiveness of Webcam Indicator Lights

Rebecca S. Portnoff[1], Linda N. Lee[1],
Serge Egelman[1,2], Pratyush Mishra[1], Derek Leung[1], and David Wagner[1]

[1]University of California, Berkeley, CA
{rsportnoff,lnl,egelman}@cs.berkeley.edu, {pratyushmishra,derek.leung}@berkeley.edu
[2]International Computer Science Institute, Berkeley, CA, egelman@icsi.berkeley.edu

ABSTRACT

Most laptops and personal computers have webcams with LED indicators to notify users when they are recording. Because hackers use surreptitiously captured webcam recordings to extort users, we explored the effectiveness of these indicators under varying circumstances and how they could be improved. We observed that, on average, fewer than half of our participants (45%) noticed the existing indicator during computer-based tasks. When seated in front of the computer performing a paper-based task, only 5% noticed the indicator. We performed a followup experiment to evaluate a new indicator and observed that adding onscreen glyphs had a significant impact on both computer-based and non-computer-based tasks (93% and 59% noticed the new indicator, respectively). We discuss how our results can be integrated into current systems, as well as future ubiquitous computing systems.

Author Keywords

Privacy Indicators; Ubiquitous Computing; Usable Security

ACM Classification Keywords

K.6.5. Management of Computing and Information Systems: Security and protection; H.5.2. Information Interfaces and Presentation (e.g. HCI): User Interfaces

INTRODUCTION

As we enter the age of wearable and ubiquitous computing, more and more consumer computing devices will accept continuous input via audio and/or video sensors. These devices allow applications to perform a wide range of actions, from recognizing objects in the user's environment to parsing voice commands. Similar to smartphone platforms [26], ubiquitous computing platforms will need permission mechanisms to allow users to regulate *how* specific applications access sensitive data, and privacy indicators to communicate *when* that data is accessed. In order for us to understand the design space of these privacy indicators, we examined the effectiveness of similar privacy indicators that are already sufficiently pervasive: webcam recording indicators.

For several years now, laptop sales have surpassed desktop sales [21], and with few exceptions, it is standard for a new laptop to come equipped with a built-in webcam. These webcams face the user and have indicator LEDs to communicate when the webcam is recording. Ideally, the user will notice the indicator, understand that a recording is being made, and take defensive actions in the event that the webcam is recording without the user's consent. Anecdotal evidence suggests that these assumptions are incorrect [13].

Remote Administration Tools (RATs) allow hackers to control an unsuspecting user's computer remotely, allowing them to execute programs, send taunting messages, or eavesdrop via the webcam and microphone [4]. In some cases, hackers have used videos of victims in various states of undress as part of "sextortion" plots: the perpetrator threatens to publicly post the captured videos and/or photos unless the victim pays a ransom [3]. The most famous case of this involved a high school classmate of Miss Teen USA who surreptitiously captured photos of her naked in her bedroom [19]. Unauthorized access to laptop webcams is not just limited to extortionists, however. In 2010, the Lower Merion School District in Pennsylvania paid a settlement to victims after it was reported that school administrators were spying on students in their homes using school-provided laptops [30].

While users can buy stickers to cover up the webcams to prevent unauthorized video capture [25], we wanted to explore the effectiveness of current webcam LED indicators and examine ways in which they could be improved, so that our findings can be applied to future technologies. We performed a series of experiments to quantify how often users are likely to take notice when their webcams unexpectedly turn on. First, we turned on the webcam unexpectedly while participants were using the computer, to see how often they noticed and whether this was affected by their activities. Next, we studied the effectiveness of a new indicator. In this work, we contribute the following:

- We show that in our laboratory environment, a minority of participants (45%) noticed an illuminated webcam LED indicator when performing a computer-based task, regard-

CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea.

ACM 978-1-4503-3145-6/15/04...$15.00.
http://dx.doi.org/10.1145/2702123.2702164

less of what that task specifically was. When performing tasks not on the computer, but in its proximity, only 5% of participants noticed the webcam LED.
- We show that the use of full-screen glyphs significantly increases the likelihood that participants notice the webcam indicator: both when performing computer-based tasks (93%) and non-computer-based tasks (59%).

RELATED WORK

In this section, we present related work on webcam indicator attacks, privacy/security indicator design and evaluation, and privacy considerations for ubiquitous computing.

Attacks on Webcam LEDs

In order for users to notice and comprehend privacy indicators, they must be reliably present. Although our work assumes that webcam LEDs will reliably illuminate when a recording is being made, recent studies demonstrate that this assumption is not always correct. Most webcam LEDs are wired in the same logical connection as the webcam, so that the LED will turn on with the webcam. This varies from device to device, however, with some indicators controlled by software [34]. Nevertheless, because of this, many people incorrectly believe that it is not possible to disable the indicator without attacking the hardware.

Recent research, however, shows that an attacker can exploit software vulnerabilities to cause some of these indicators to malfunction. Broker *et al.* demonstrated an attack on webcam firmware that enables video capture without turning on the webcam LED on older versions of Mac laptops [9]. While these attacks are troubling, we assume that devices will eventually be designed so that indicators cannot be disabled; research on understanding whether the indicators are effective at communicating risk to users is still necessary.

Indicators and Warnings

Cranor discusses various evaluation criteria for indicators and warnings [16], such as how an indicator interacts with other indicators, and whether users notice, understand, and follow its recommendations, both after first exposure and then repeated exposures. Other considerations include how warnings are displayed [23], when they are displayed [24], and how they make use of icons and signal words [2].

Poorly designed indicators not only fail to communicate the appropriate message to users, but can have other unintended negative consequences, such as desensitization, habituation, or annoyance [39]. They can also create a false sense of security [10]. For example, when people notice the HTTPS lock icon (and they tend not to [40]) they often incorrectly assume that it indicates a secure website, rather than a secure connection [29]. Users also do not change their behavior when this indicator is absent [38]. When designing privacy and security indicators, it is important to examine these potential pitfalls.

Privacy Concerns for Ubiquitous Sensing

Wearable devices and ubiquitous sensing platforms are moving towards automated capture and access [1]. More and more often, people will interact with sensors while carrying out daily activities, from a myriad of sources and for a variety of reasons: "lifelogging" devices to record their daily lives [31, 18], memory augmentation devices [14, 17, 32], smart homes that optimize living conditions [12, 11, 22], devices that create augmented reality environments [7, 6], and even devices integrated into clothing [5].

The ubiquitous capture and storage of information naturally raises concerns about the preservation of privacy [35]. Privacy in the field of ubiquitous computing relies on principles including notice, choice, and consent [33]. Certain privacy problems stem from poor feedback mechanisms [8, 20]: indicators failing to reliably inform people *when* they are being captured and *what* information is being saved.

Clearly, there is a critical need for effective privacy indicators that users will notice and understand. Research has suggested that notifications in a user's peripheral field of vision may be acceptable for certain cases [15]. It is not clear, however, whether this is an effective strategy for every or even most privacy and security notifications.

Although significant work has been done to explore privacy/security indicator designs, researchers have not yet focused specific attention on the ubiquitous webcam LED.

AWARENESS AND PERCEPTIONS

To quantify the problem of "webcam spying," we first conducted an online survey. Our goal was to better understand whether people are likely to be at risk, their awareness of the danger, and how many claim to have already been victimized.

Methodology

We recruited 500 participants on December 9th, 2013 via Amazon's Mechanical Turk. We restricted participants to those over 18 years old residing in the U.S. All participants stated that they owned a laptop or desktop computer with either an external or internal webcam. We asked questions about participants' webcam use and their understanding of the indicator LED. The questions fell into three categories:

1. *Behavior*: The types of participants' webcams and whether they obscure them when not in use.
2. *Risk Awareness*: Whether participants believe that webcam spying is possible.
3. *Victimization*: Whether participants have noticed the webcam LED previously come on against their wishes.

The entire survey took approximately 7 minutes to complete, upon which we compensated them $1.

Results

After removing 8 incomplete responses, our sample consisted of 492 participants (64% male and a median age range of 26-30). Two researchers independently coded 1,476 open-ended responses (94.3% agreement), discussed any disagreements, and resolved them to reflect unanimous agreement.

Behavior

We asked laptop-owning participants whether they "always," "sometimes," or "never" close their laptop lids when not using it. We found that 45% reported "always" doing so,

whereas another 36% reported doing so "sometimes." We also asked whether participants were comfortable doing any of the following in front of an open laptop:

- Going to the restroom
- Eating meals
- Changing clothes
- Talking to friends
- Taking a shower

We found that 28% were comfortable using the restroom, 85% were comfortable eating meals, 41% were comfortable changing clothes, 80% were comfortable talking to a friend, and 18% were comfortable taking a shower. Because we previously subjected participants to questions regarding webcams before answering this question, these numbers are likely under-reported and therefore represent lower bounds. While we are not aware of any peer-reviewed literature on the matter, an industry-commissioned survey reports that 44% of respondents use their laptops in the bedroom and 8% in the bathroom [37]. Our data suggests that large groups of users practice behavior that puts them at risk of webcam spying.

Risk Awareness

We asked participants whether they thought it would be possible for a hacker to spy on them through their webcam, and to indicate why or why not. We found that 13% did not think it would be possible, and 19% were unsure. The open-ended responses ranged in technical fluency, ranging from distrust of the notion of foolproof technologies to discussing how root access could allow an attacker to control a device.

Victimization

Nineteen participants reported that their webcam LED turned on when they were not using it. Almost all of them (18 of 19) believed this was normal behavior or just due to human error, while one participant was the victim of ransomware, stating:

> *"I had contracted a virus on my laptop the FBI classifies as 'ransomware.' It tells you you cannot access your computer unless you wire money to an account, and it turns on the webcam to frighten people. I was surprised and very anxious, and I responded by covering my webcam with black electrical tape."* (P30)

Our survey showed that many people practice habits that increase their risk and that they are unaware of the danger. In the following section, we describe our empirical evaluation of the common webcam LED, in terms of the proportion of users who are likely to notice it when it unexpectedly illuminates, and whether this varies based on the task being performed.

LABORATORY EXPERIMENT

We conducted a laboratory experiment to examine the extent to which people notice and understand current webcam LEDs, as well as the extent to which their activities impact the likelihood of noticing the LEDs. We explored this because an attacker with remote access to a victim's webcam would also be able to see what the victim is doing, and potentially use this information to increase attack effectiveness. In this section, we provide details of our methodology and results.

Methodology

We conducted an experiment with 98 participants. All participants used Toshiba Tecra R850 laptops, which use a blue LED next to the webcam lens to indicate when the webcam is recording. We examined whether participants noticed the webcam LED turning on when performing a computer-based task, as well as a non-computer-based task within close proximity of the webcam (i.e., answering a written questionnaire).

Procedure

We conducted each session in a laboratory space at our university that consisted of 36 laptops, in 6 rows, with cubicle walls separating each laptop. No more than 15 participants attended each session. We distanced each participant from every other participant by at least one desk, by only using every other laptop in each staggered row. Our goal was to prevent participants from viewing each other's laptops.

Upon arriving, participants sat down at laptops of their choosing, where consent forms were present. Once participants read and signed the consent forms, the researcher outlined participants' tasks and explained that the purpose of the study was to see how people perform various tasks on a computer. Again, the true purpose of the study was not revealed. Each session proceeded as follows:

1. Participants answered the 30-item Barratt Impulsiveness Scale [36], which was used as a distraction to make them comfortable with the environment.
2. Participants performed one of four randomly-assigned computer-based tasks lasting 10-15 minutes. At some random point after 5 minutes, the webcam made a 10 second recording. Participants were prevented from advancing to the next task until at least 10 minutes had elapsed. There were four different types of computer-based tasks:
   - **Reading**: Participants read a provided passage [27]. We told them that they would be asked questions about the reading, so they should read it thoroughly.
   - **Essay**: Participants saw a previous year's SAT writing prompt. We told them to write an essay based on the prompt as part of a college or job application.
   - **Game**: Participants played the 2048 game.[1] We instructed them to try to get as high a score as possible in 10-15 minutes.
   - **Video**: Participants watched a TED talk,[2] which we told them they would be asked questions about.
3. Each participant took the Cognitive Reflection Test on a printed sheet of paper on the desk in front of the laptop [28]. At some random point after 60 seconds into the task, the webcam made a 10 second recording. Participants were prevented from advancing to the exit survey until at least 2 minutes had elapsed.
4. Each participant filled out an exit survey on the computer.
5. Upon completing the exit survey, we debriefed participants. We gave each participant a re-consent form, which would allow us to use the webcam video in our analysis, and paid them with $35 debit cards.

[1] http://gabrielecirulli.github.io/2048/

[2] https://www.youtube.com/embed/xMj_P_6H69g

	Noticed light	
Computer Task	27.6%	n = 98
Reading	46.4%	n = 28
Essay	25.0%	n = 28
Game	25.0%	n = 20
Video	9.0%	n = 22
Written Task	0%	n = 98

Table 1. Unprompted responses: the number of participants who described noticing the webcam LED turn on during each task.

	Light turned on	Recording	
Computer Task	44.9%	33.7%	n = 98
Reading	53.6%	32.1%	n = 28
Essay	35.7%	32.1%	n = 28
Game	45.0%	30.0%	n = 20
Video	45.5%	40.9%	n = 22
Written Task	5.1%	5.1%	n = 98

Table 2. Prompted responses: the number of participants who selected either that the webcam LED turned on or the webcam began recording.

	Made Eye Contact	
Computer Task	48.9%	n = 94
Reading	63.0%	n = 27
Essay	40.7%	n = 27
Game	55.6%	n = 18
Video	36.4%	n = 22
Written Task	4.26%	n = 94

Table 3. Participants observed making eye contact with the webcam.

Recruitment

We placed an online recruitment advertisement on Craigslist in June of 2014, under the "writing/editing" jobs section for our city and surrounding cities. The advertisement stated that the study was about how people perform various tasks on a laptop. Those interested in participating filled out an online screening survey in which they provided information about their age, gender, laptop make and model, amount of time using their laptop, various ways they have used their laptop (social networking, video recording, playing games, making video calls, making online purchases), contact information, and availability. We screened out those who were under 18 years of age or who had a laptop that did not have a webcam.

We recruited 98 participants who showed up for sessions lasting 30-60 minutes. Of our 98 participants, 55 were female (56%), and ages ranged from 18 to 72 ($\mu = 37.9$, $\sigma = 15.4$).

Results

Our primary goal was to assess the effectiveness of the webcam LED. We found that the majority of participants did not notice it turn on during either task, and many did not understand what it indicated, even when they did notice it. In this section, we provide details for whether participants noticed the webcam LED, our efforts to corroborate the self-reports using the captured videos, whether any of the computer-based task conditions influenced the participants to notice the webcam LED more or less, and participants' understanding of the purpose of the webcam LED.

Noticing the Indicator

We determined whether participants noticed the webcam LED through multiple exit survey questions. First, we asked them if anything unexpected had occurred as they completed the computer-based task and the written task. We used open-ended formats so as to not prime them (i.e., we made no mention of the webcam). We accepted responses that reported the webcam or the LED turning on as evidence that they noticed it. Only 27.6% (27 of 98) of participants reported noticing it during the computer-based task (Table 1). No participants reported noticing the webcam LED during the written task.

On the next page of the exit survey, we asked participants which (if any) of the following occurred during the computer-based task, and then during the written task. For each participant, we randomized the order of the following options:

- The webcam began recording
- A light above the screen turned on
- The desktop background changed
- An unexpected sound played
- The screen flickered
- The computer rebooted
- None of the above

Once prompted, the rate at which participants reported noticing the light increased. During the computer-based task it increased to 44.9% (44 of 98), whereas during the written task, it increased from 0% to 5.1% (5 of 98).

To corroborate our exit survey data, we examined the webcam recordings. Four of our 98 participants declined to give us permission to use their recordings. Three researchers independently coded all 188 recordings (two per participant) to judge whether each participant made eye contact with the camera (i.e., an indication that they were looking at it), and if so, at what point in time during the 10 second recording. The researchers then resolved any disagreements, so that final codings were unanimous. Prior to achieving consensus, they disagreed on 26 instances (86.2% agreement).

Based on the recordings, 48.9% (46 of 94) of participants noticed the webcam LED during the computer-based task, and 4.26% (4 of 94) noticed it during the written task (Table 3). During the computer-based task, of the 46 participants who we observed making eye contact with the webcam, all of them did so within the first four seconds; 71.7% (33 of 46) noticed it immediately (Figure 1). During the written task, all four of them noticed within the first seven seconds.

Using our three different metrics (unprompted responses, prompted responses, and recordings), we concluded that 27%-49% of participants noticed the webcam LED during the computer-based task, whereas $\leq 5\%$ noticed it during the written task. Since the recordings and prompted responses were similar, we did not consider the recordings further.

Task Influence

We examined the effects of participants' tasks on noticing the webcam LED. We analyzed differences between computer-based tasks and the written task (within-subjects), as well as between specific computer-based tasks (between-subjects).

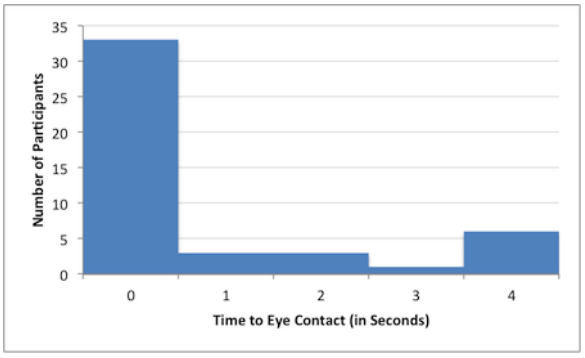

Figure 1. Time into recording at which participants made eye contact.

We determined using McNemar's test that participants were significantly more likely to notice the indicators when performing the computer-based task, based on both the unprompted ($p < 0.0001$; $\chi^2 = 25.037$) and prompted ($p < 0.0001$; $\chi^2 = 33.5814$) responses. Using either measure, we observed relatively large effect sizes ($\phi_{unprompted} = 0.505$, $\phi_{prompted} = 0.585$), which indicates that participants were more likely to notice the webcam LED while performing a task on the computer, rather than merely in its proximity.

When it came to differences between specific computer-based tasks, we did not observe statistically significant results when examining both unprompted ($\chi^2(3) = 5.917, p < 0.116$) and prompted ($\chi^2(3) = 1.000, p < 0.8013$) responses. Thus, we conclude that the specific computer-based tasks that we evaluated had no observable effect on whether participants noticed the indicator.

Understanding the Webcam LED

We examined whether participants understood that the blue webcam LED indicated that the webcam was recording by observing their responses to the multiple-choice prompting question. For the computer-based task, we found that 45.5% (20 of 44) of the participants who reported noticing a light above the screen *only* reported the light, and not also that the webcam recorded them. For the written task, this rate was 40.0%. While it is impossible to conclude with certainty without directly asking the question, these results may suggest a comprehension problem with the webcam LED: even when the participants did notice the webcam LED turning on, up to 45.5% of them may not have understood what it meant. Alternately, it is possible that they did not know that they could select multiple options (despite the question instructions allowing them to do so), and therefore selected the first one that applied, without reading the other possibilities.

The results of our experiment demonstrate that the webcam LED needs to be more noticeable, and potentially more understandable. In the following section, we describe a follow-up experiment to test a possible alternative indicator: a full-screen flashing translucent camera glyph.

MITIGATION

We created a new mitigation whereby every time the webcam turned on, a full-screen red translucent camera glyph appeared in the center of the screen and blinked three times

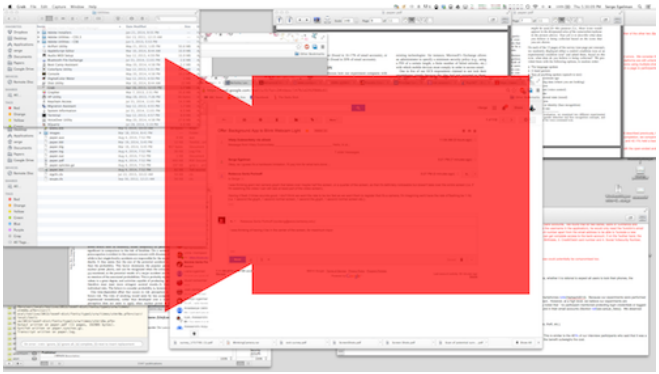

Figure 2. Full screen image of the red camera glyph.

(Figure 2). The glyph then shrunk into the upper right hand corner where it continued blinking once per second. In total, the red translucent camera glyph blinked for 10 seconds (3 seconds full screen, and 7 seconds in the upper right hand corner). We intentionally made the glyph translucent so that it would not occlude other items on the screen (to account for the case when the user is expecting the webcam to be on).

Methodology

We randomly assigned participants to one of two between-subjects conditions, which varied based on the webcam indicator shown: *control* group participants viewed the blue webcam LED, whereas *experimental* group participants additionally viewed the red camera glyph described at the beginning of this section (Figure 2).

Our followup experiment followed the same protocol as our initial laboratory experiment, with a few exceptions. Given the lack of noticeable effect of different computer-based tasks on participants noticing the webcam LED, we focused on just the video task. Additionally, given that self-reported noticing of the webcam LED was found to be reliable, we chose not to save webcam recordings of participants.

We recruited 81 participants in the exact same manner as our first experiment. In total, 46 were female, and ages ranged from 18 to 65 ($\mu = 33.7$, $\sigma = 13.1$). Of the 81 participants, 37 were randomly assigned to the control group. We observed no statistically significant demographic differences between participants in the control and experimental groups.

Results

We found that using the red camera glyph substantially increased the rate at which participants reported noticing the indicator. We also found that their understanding of what the warning indicated diminished, but not by a statistically significant amount. In this section, we compare the rates at which test group and control group participants noticed and understood the meanings of their respective indicators.

Noticing the Red Camera Glyph

We asked participants whether anything unexpected had occurred during the computer-based task or the written task. We accepted any statement that reported the webcam turning on or the red camera glyph appearing as evidence that

	Noticed	
Computer Task		
Experimental	65.9%	n = 44
Control	16.2%	n = 37
Written Task		
Experimental	40.9%	n = 44
Control	2.7%	n = 37

Table 4. Unprompted responses: the number of participants who described noticing the indicator appear/turn on.

	Indicator	Recording	
Computer Task			
Experimental	93.2%	25.0%	n = 44
Control	40.5%	37.8%	n = 37
Written Task			
Experimental	59.1%	18.2%	n = 44
Control	5.41%	5.41%	n = 37

Table 5. Prompted responses: number of participants who selected either that the indicator appeared or that the webcam began recording.

they noticed the red camera glyph. We observed that 65.9% (29 of 44) of participants in the experimental group reported noticing the camera glyph appear (Table 4). In contrast, only 16.2% (6 of 37) of control group participants reported noticing the webcam LED. This difference is statistically significant ($p < 0.0001$; two-tailed Fisher's exact test), with a very large effect size ($\phi = 0.500$).

When asked the same question for the written task, over 40% of the experimental group participants reported noticing the red camera glyph, whereas only one participant in the control group reported noticing the webcam LED turn on (see Table 4). This difference was also statistically significant ($p < 0.0001$; two-tailed Fisher's exact test), with a very large effect size ($\phi = 0.449$).

When prompted, participants saw the same seven options as in the first laboratory experiment, but with an added option: "a red camera image appeared on the screen." When prompted, 93.2% (41 of 44) of experimental group participants reported noticing the red camera glyph during the computer-based task (Table 5). For the control group, fewer than half reported noticing the webcam LED. This difference was statistically significant ($p < 0.0001$; two-tailed Fisher's exact test), with a very large effect size ($\phi = 0.568$).

When asked the same question for the written task, over half of our participants in the experimental group reported noticing the red camera glyph, whereas only two control group participants reported noticing the webcam LED turn on (Table 5). This difference was statistically significant ($p < 0.0001$; two-tailed Fisher's exact test), with a very large effect size ($\phi = 0.562$).

We used McNemar's test to determine that participants were significantly more likely to notice the red camera glyph when performing the computer-based task than the written task, based on both the unprompted ($p = 0.0003$; $\chi^2 = 13.067$) and prompted ($p = 0.0026$; $\chi^2 = 9.091$) responses. Using either measure, we observed relatively large effect sizes ($\phi_{unprompted} = 0.402$, $\phi_{prompted} = 0.335$), which indicates that participants were more likely to notice the red camera glyph while performing a task on the computer, rather than merely in its proximity.

In all cases, the rate at which participants noticed the indicator was significantly better when viewing the red camera glyph than when viewing the standard webcam LED.

Understanding the Red Camera Glyph

We were curious to see whether or not using the red camera glyph as the indicator vs. the webcam LED changed the rate at which participants understood that the webcam was recording. When looking at the unprompted responses for the test group, of the participants who noticed the glyph, but did not explicitly state it was a camera, most reported seeing some combination of red blocks, shapes and symbols:

> *"[I saw] a few red arrows or shapes flashed on the screen."* (P2)

> *"[I saw] flashes of a faint red arrow across the screen."* (P3)

> *"...a couple red flashing symbols appeared on the screen."* (P19)

We found that 25.0% (11 of 44) of experimental group participants reported that the webcam began recording during the computer-based task, compared to 37.8% (14 of 37) of participants in the control group (Table 5). For the written task, the corresponding rates were 18.2% (8 of 44) and 5.41% (2 of 37), respectively.

In both cases, the difference was not statistically significant: ($p = 0.236$, two-tailed Fisher's exact test) and ($p = 0.101$, two-tailed Fisher's exact test) for the computer-based task and written task, respectively. These results seem to indicate that the number of participants who understood our warning mechanism was essentially the same as the number that understood the standard webcam LED.

The results of our experiment demonstrate that our red camera glyph indicator significantly outperformed the standard webcam LED in terms of participants' rate of noticing the indicator, with similar comprehension rates. In the next section, we analyze the results of our exit survey to see whether any correlations can be found between participants' previous experiences noticing their personal webcam turning on unexpectedly, and noticing the indicator in our experiments.

EXIT SURVEY

In this section, we examine participants' previous experiences with having their personal webcams turn on unexpectedly, their security and privacy concerns, and their security behavior regarding their webcams, as gathered from our exit survey.

Experienced Webcam Turning on Unexpectedly

Of the 179 participants from our two lab experiments, 13.4% (24 of 179) had experienced a webcam turn on unexpectedly some time in the past (i.e., prior to this study), 79.9% (143 of 179) had not, and the remaining 6.70% (12 of 179) were unsure if this had ever happened.

We compared participants' prior experiences with their behaviors in the laboratory, excluding those who were unsure whether their webcams had ever turned on unexpectedly. Of the 24 who claimed to have experienced it in the past, when prompted, 20.8% (5 of 24) reported noticing the indicator during the computer-based task; of the 143 who had not experienced it, 56.6% (81 of 143) reported the same. This difference was statistically significant ($p < 0.0025$; two-tailed Fisher's exact test) with a medium effect size ($\phi = 0.251$). For the written task, 8.33% (2 of 24) reported noticing the indicator; of the 143, 16.8% (24 of 143) reported the same. However, this difference was not statistically significant.

In other words, for the computer-based task, it seems that those who had prior experiences with webcams turning on unexpectedly were *less* likely to notice it happen in the laboratory, which seems counterintuitive. It seems likely that some other confounding factor is in effect here. It could be the case that previous victims have become accustomed to the protection their personal security measures provide, and as a result do not pay as much attention to the webcam indicator. We found that 29.2% (7 of 24) of participants who have previously noticed their webcams turn on unexpectedly claim to now cover the camera lens of their home computer/laptop when not in use, as compared to 9.79% (14 of 143) of those who have not. The difference was statistically significant ($p = 0.0157$, two-tailed Fisher's exact test) with a medium effect size ($\phi = 0.2050$), though this effect may not be statistically significant upon correcting for multiple testing (e.g., using the Bonferroni correction).

Security/Privacy Concerns

When asked to state any and all possible consequences if the webcam on their home computer/laptop unexpectedly recorded them and the video became public, most participants offered multiple responses. The most frequent response was "violation of privacy." As one participant poignantly stated:

> *"I would look foolish, I'm sure. People would see me at my best and at my worst. They would see my daughter and husband when they weren't expecting it. They would see us in our most intimate moments. I would be devastated that our privacy was violated so completely. It would be like someone broke into our home and stole our secrets."* (P90)

Many participants stated concern over intimate moments being made public:

> *"There would be a sex video online somewhere, I would be seen completely naked from changing out of the shower, or I would be sleeping in my bed."* (P127)

> *"I'd feel really violated, I mean sometimes I'm sitting in front of my computer naked, or smoking weed, and I'd be really uncomfortable with video like that becoming public."* (P150)

> *"The camera might... record me masturbating."* (P156)

> *"I live in a studio with my boyfriend, so the video might end up on a porn site."* (P188)

A smaller subset of participants were more worried about what other data/information a hacker might be able to gain access to while spying on them:

> *"Not sure. Possibly home burglary because they can see what's in the house."* (P10)

> *"...identity theft or loss of money."* (P34)

> *"I'm more concerned about this being a warning sign that someone has access to all the information on my computer..."* (P51)

Security Behavior

When asked to state what participants would do if the webcam on their home computer/laptop began recording unexpectedly, the most frequent response was "cover the camera lens," followed closely by "seek outside help." Almost every participant stated that they would try some way to "fix" the problem, even if they could not state exactly what steps they would take:

> *"I would try to determine the cause of the unexpected recording and then take measures to prevent it from happening in the future."* (P21)

> *"I would investigate and see if I could stop [it]..."* (P78)

> *"I would try to figure out how to stop it from doing it and try to figure out how to not let that happen again."* (P188)

Some participants stated they would resort to more extreme measures:

> *"Scan, and if necessary, bomb the harddrive."* (P17)

> *"Disconnect it when not in use, possibly destroy it."* (P44)

> *"Throw it out the window..."* (P63)

It is clear to see from these responses that participants value their security and privacy, and are troubled by the thought of someone watching them without their permission.

LIMITATIONS

After completing our experiments, we realized that by not randomizing the order in which the computer task versus the written task was performed, we could not guarantee that there was no learning or habituation effect. Although this was an unfortunate oversight, we found that for everything but the mitigation experimental group, it had no observable effect on our results. We performed Phi correlations between the rates of noticing the indicators between the two tasks and found no statistically significant correlations for the first laboratory experiment ($p < 0.49$, $\phi = 0.07$) or for the followup mitigation experiment in the control group ($p < 0.083$, and $\phi = 0.29$). For the experimental group (i.e., the red

camera glyph), we found a potentially significant correlation ($p < 0.029$, $\phi = 0.33$), though upon correcting for multiple testing, it is unlikely to remain statistically significant. Given these results, there is no evidence to suggest that this oversight impacted our conclusion regarding the utility of the webcam LED as a warning mechanism, or the improvement gained by the red glyph.

DISCUSSION

In this section, we discuss the space of future mitigation research as we see it, as well as more sophisticated attacks.

Mitigations

While we found the red camera glyph, taken as a whole, to be significantly more effective than the status quo, it is by no means the only solution (or necessarily the best). More work is needed to show how each change contributed individually, as the red camera glyph differed in size, color, and movement, as compared to the existing webcam LED. More broadly speaking, more work is needed to explore other potential design improvements. We see two main categories of study which remain to be explored in regard to webcam indicators, as well as privacy indicators in general:

1. Designing indicators that users will notice
2. Improving user understanding of the indicators

Noticeable Indicators

We see two main classes of potential indicators for the webcam, namely hardware-based and software-based indicators. Hardware-based solutions are preferable, as they prevent a hacker who has used a root exploit to gain control of the machine from accessing the webcam without triggering the indicator. Existing webcam LED indicators are typically implemented in hardware. For our experiments, we implemented the red camera glyph in software, which means that an attacker with root access could disable it. Any real-life implementation of the red camera glyph as an indicator would need to be implemented in hardware, like the standard webcam LED currently is.

One natural way to expand on the current webcam LED is to have it flash/blink, rather than hold steady. The most basic set up would be to have the webcam LED blinking constantly throughout the duration of the recording, though this might be distracting or irritating for users. Alternatively, the LED could blink when the webcam is first turned on, in order to draw the user's attention to it immediately, and after some amount of time, it could return to a steady light. The LED could also blink intermittently throughout the recording; this might be useful in drawing the user's attention to the LED even when the user did not initially notice it.

In a pilot experiment, we explored whether simply blinking the webcam LED would be sufficient. While blinking the LED did not yield significantly improved results over the control condition, that may have been because the frequency of blinking was only 0.5 Hz. We were not able to increase this speed due to hardware limitations. It seems possible that with a faster blinking speed, more users might notice the LED.

Exploring a larger variety of computer-based tasks could also be worthwhile. Determining whether users are more likely to notice the webcam indicator when performing tasks that are menial and/or automatic vs. active and require conscious attention could allow researchers to design indicators that have a varying signal size based on task. For example, if the webcam turned on while the user was performing a menial or automatic task, the indicator signal would be smaller; if it turned on while the user was performing a task requiring conscious attention and focus, the signal would be larger.

Another challenge is to to help users notice the indicator when they are not using their computers, but are in the same room as their computers. This challenge is especially important because it includes the scenario of when a person is in a compromising or intimate situation. A brighter webcam LED might help in this circumstance (e.g., a flash LED). Using an audio signal could also be helpful in this scenario, although not for people who regularly leave their headphones plugged in, mute their computer, or have hearing problems.

Improving Understanding

It is critically important for people to comprehend what the warning signal means: without understanding, the indicator is useless. One possibility for improving comprehension would be to display a one-time-only explanation of the warning that appears the first time a person uses the webcam, and never again. This solution would not be dependent on a user's prior knowledge. However, it is unclear whether or not users would actually pay attention to the explanation. Given that current users are not used to a message appearing when they turn their webcams on, it is possible that users may automatically close it without paying attention, or even believe the message indicates the presence of malware on their machine.

Over time, people may come to learn the meaning of a new indicator such as our red camera glyph, simply because it always appears each time the webcam is in use. However, even time and experience are not a perfect solution: people have used the presence of a light as an indicator that video is recording for ages, and yet people still have confusion as to what exactly the webcam LED indicates. One possible alternative is to change the form of the webcam LED light; rather than having a small circle of light, the LED could be designed to emit light in the shape of a video camera. It is possible that the combination of the traditional LED light and the video camera shape could fix what time and experience have not.

Sophisticated Attacks

There are a number of ways in which attackers could attempt to spy on users through their webcams without the users realizing. One natural method would be to distract users from looking in the direction of the webcam LED when the webcam turns on, possibly by drawing their eye to somewhere else on the screen with a pop-up or some other distraction. Other techniques could use social engineering: an attacker could implement a false webcam driver update message that appears whenever he turns on the victim's webcam. The intention of the message would be to lull the user into a false sense of security, so even if she notices that the webcam is on and recording, she believes it is part of the update process.

Attackers could also use other features to infer when users are away from their computers, and are less likely to notice the webcam LED turning on. In the most trivial scenario, an attacker could wait until there is no activity on the computer to turn the webcam on. This could get more complex: a clever attacker could learn his victim's schedule and habits of computer usage to learn the optimal time to turn the webcam on.

An attacker could potentially pick up this kind of information by remotely turning on the microphone. This sensor currently has absolutely no indicator for when it is turned on. This is a very serious concern, given the security and privacy implications of a malicious attacker listening in on a user's daily life and activities.

CONCLUSION

We demonstrated that the current webcam LED is not effective as an indicator to communicate when the webcam is recording. We created our own indicator which significantly improved the rate at which participants noticed it, both during computer-based tasks and for non-computer-based tasks, without significantly decreasing their understanding. We analyzed our participants' previous experience with the webcam on their personal computer/laptop turning on unexpectedly, finding that this previous experience inversely correlated to noticing the webcam LED in our experiments. Based on our experimental results, we offer an initial step towards designing better webcam indicators for user. Finally, we outline the space of future mitigation research as we see it, to make sure users both notice and understand future privacy indicators.

ACKNOWLEDGEMENTS

This work was supported by the Intel Science and Technology Center for Secure Computing (ISTC-SC), NSF under award CNS-1318680, and AFOSR under MURI award FA9550-12-1-0040. We would like to thank Vitaly Dubnovitsky for assistance implementing the webcam glyph.

REFERENCES

1. Abowd, G. D., and Mynatt, E. D. Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction (TOCHI) 7*, 1 (2000), 29–58.
2. Amer, T., and Maris, J.-M. B. Signal Words and Signal Icons in Application Control and Information Technology Exception Messages-Hazard Matching and Habituation Effects. *Journal of Information Systems 21*, 2 (2007), 1–25.
3. Anderson, N. How an Omniscient Internet "Sextortionist" Ruined the Lives of Teen girls. **http://arstechnica.com/tech-policy/2011/09/how-an-omniscient-internet-sextortionist-ruined-lives/**, September 7 2011. Accessed: September 6, 2014.
4. Anderson, N. Meet the Men Who Spy on Women through Their Webcams. **http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/**, March 10 2013. Accessed: September 5, 2014.
5. Anliker, U., Lukowicz, P., Troester, G., Schwartz, S. J., and DeVaul, R. W. The WearARM: Modular, High Performance, Low Power Computing Platform Designed for Integration into Everyday Clothing. In *Wearable Computers, 2001. Proceedings. Fifth International Symposium on*, IEEE (2001), 167–168.
6. Azuma, R., Baillot, Y., Behringer, R., Feiner, S., Julier, S., and MacIntyre, B. Recent Advances in Augmented Reality. *Computer Graphics and Applications, IEEE 21*, 6 (2001), 34–47.
7. Azuma, R. T., et al. A Survey of Augmented Reality. *Presence 6*, 4 (1997), 355–385.
8. Bellotti, V., and Sellen, A. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93*, Springer (1993), 77–92.
9. Brocker, M., and Checkoway, S. iSeeYou: Disabling the MacBook Webcam Indicator LED. In *Proceedings of the 23rd USENIX Security Symposium*, USENIX Association (2014).
10. Cannella, S., Polivy, D. J., Shin, M., Straub, C., and Tamassia, R. Secure Visualization of Authentication Information: A Case Study. In *Visual Languages and Human Centric Computing, 2004 IEEE Symposium on*, IEEE (2004), 35–37.
11. Chan, M., Campo, E., Estève, D., and Fourniols, J.-Y. Smart Homes—Current Features and Future Perspectives. *Maturitas 64*, 2 (2009), 90–97.
12. Chan, M., Estève, D., Escriba, C., and Campo, E. A Review of Smart Homes—Present State and Future Challenges. *Computer methods and programs in biomedicine 91*, 1 (2008), 55–81.
13. Check Point Software Technologies Ltd. Are You Being Watched Through Your Webcam? **http://www.zonealarm.com/blog/2013/10/are-you-being-watched-through-your-webcam/**, October 2 2013. Accessed: September 6, 2014.
14. Chen, Y., and Jones, G. J. Augmenting Human Memory Using Personal Lifelogs. In *Proceedings of the 1st Augmented Human International Conference*, ACM (2010), 24.
15. Costanza, E., Inverso, S. A., Pavlov, E., Allen, R., and Maes, P. Eye-q: Eyeglass Peripheral Display for Subtle Intimate Notifications. In *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, ACM (2006), 211–218.
16. Cranor, L. F. What Do They Indicate?: Evaluating Security and Privacy Indicators. *Interactions 13*, 3 (2006), 45–47.

17. DeVaul, R. W., Corey, V. R., et al. The Memory Glasses: Subliminal vs. Overt Memory Support with Imperfect Information. In *2012 16th International Symposium on Wearable Computers*, IEEE Computer Society (2003), 146–146.
18. Dickie, C., Vertegaal, R., Fono, D., Sohn, C., Chen, D., Cheng, D., Shell, J. S., and Aoudeh, O. Augmenting and Sharing Memory with eyeBlog. In *Proceedings of the the 1st ACM workshop on Continuous archival and retrieval of personal experiences*, ACM (2004), 105–109.
19. Dobuzinskis, A. California Man Agrees to Plead Guilty to Extortion of Miss Teen USA. **http://www.reuters.com/article/2013/10/31/us-usa-missteen-extortion-idUSBRE99U1G520131031**, October 31 2013. Accessed: September 5, 2014.
20. Dourish, P., Grinter, R. E., De La Flor, J. D., and Joseph, M. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing 8*, 6 (2004), 391–401.
21. Eddy, N. Notebook sales outpace desktop sales. **http://www.eweek.com/c/a/Midmarket/Notebook-Sales-Outpace-Desktop-Sales/**, December 24 2008. Accessed: September 9, 2014.
22. Edwards, W. K., and Grinter, R. E. At Home with Ubiquitous Computing: Seven Challenges. In *Ubicomp 2001: Ubiquitous Computing*, Springer (2001), 256–272.
23. Egelman, S., Cranor, L. F., and Hong, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2008), 1065–1074.
24. Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Timing is Everything?: The Effects of Timing and Placement of Online Privacy Indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2009), 319–328.
25. Electronic Frontier Foundation. Laptop Camera Cover Set. **https://supporters.eff.org/shop/laptop-camera-cover-set**. Accessed: September 6, 2014.
26. Felt, A. P., Chin, E., Hanna, S., Song, D., and Wagner, D. Android permissions demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, ACM (New York, NY, USA, 2011), 627–638.
27. Filkins, D. What we left behind. *The New Yorker* (April 28 2014).
28. Frederick, S. Cognitive reflection and decision making. *Journal of Economic perspectives* (2005), 25–42.
29. Friedman, B., Hurley, D., Howe, D. C., Felten, E., and Nissenbaum, H. Users' conceptions of web security: A comparative study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '02, ACM (New York, NY, USA, 2002), 746–747.
30. Hill, K. Lower Merion School District and Blake Robbins Reach a Settlement in Spycamgate. **http://www.forbes.com/sites/kashmirhill/2010/10/11/lower-merion-school-district-and-blake-robbins-reach-a-settlement-in-spycamgate/**, October 11 2010. Accessed: September 9, 2014.
31. Hoyle, R., Templeman, R., Armes, S., Anthony, D., Crandall, D., and Kapadia, A. Privacy Behaviors of Lifeloggers Using Wearable Cameras. In *Ubicomp 2014: Ubiquitous Computing* (2014).
32. Kalnikaite, V., Sellen, A., Whittaker, S., and Kirk, D. Now Let Me See Where I Was: Understanding How Lifelogs Mediate Memory. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2010), 2045–2054.
33. Langheinrich, M. Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*, Springer (2001), 273–291.
34. Logitech Forum: Can I Turn off the Red LED? **http://forums.logitech.com/t5/Webcams/Can-I-turn-off-red-LED/m-p/277305#M52816**. Accessed: 2014-09-06.
35. Palen, L., and Dourish, P. Unpacking Privacy for a Networked World. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM (2003), 129–136.
36. Patton, J. H., Stanford, M. S., et al. Factor structure of the barratt impulsiveness scale. *Journal of clinical psychology 51*, 6 (1995), 768–774.
37. Rouse, R. A. Is someone watching you through your webcam? **http://campatch.com/wp-content/uploads/2012/05/CamPatch-Academy-Study-on-Webcam-Hacking-Awareness-May2012.pdf**, May 2012.
38. Schechter, S. E., Dhamija, R., Ozment, A., and Fischer, I. The Emperor's New Security Indicators. In *IEEE Symposium on Security and Privacy* (2007), 51–65.
39. Stewart, D. W., and Martin, I. M. Intended and Unintended consequences of Warning Messages: A Review and Synthesis of Empirical Research. *Journal of Public Policy & Marketing* (1994), 1–19.
40. Whalen, T., and Inkpen, K. M. Gathering Evidence: Use of Visual Security Cues in Web Browsers. In *Proceedings of Graphics Interface 2005*, Canadian Human-Computer Communications Society (2005), 137–144.