Exploring Design Directions for Wearable Privacy

Katharina Krombholz*, Adrian Dabrowski*, Matthew Smith†, and Edgar Weippl*
*SBA Research
Email: kkrombholz,adabrowski,eweippl@sba-research.org
†University of Bonn
Email: smith@cs.uni-bonn.de

***Abstract*—We explore how privacy preferences can be communicated towards disruptive cameras in privacy-sensitive spaces such as public beaches, where users are constrained in what technology they can carry and use. In order to get an informed consent between photographers and bystanders, we designed three conceptual privacy-mediating technologies: a smartphone app, a privacy-bracelet and a clothing-based approach. We then conducted 20 qualitative interviews to study peoples' privacy feelings towards disruptive cameras at a beach and in a cafe and their attitudes towards our approaches. We found that there is high demand for such tools irrespective of location and that a dedicated privacy device was preferred by most of the participants.**

I. Introduction

Mobile devices with integrated cameras have increased the number of pictures taken in public spaces. Bystanders of such devices are often photographed without their consent. This implies major challenges for digital privacy. At this time, wearable devices with continuous and unobtrusive sensing capabilities are becoming more and more popular and have the potential to become as ubiquitous as smartphones [20]. Even though Google Glass, the most controversially discussed representative of wearable cameras has not yet found its way into the communication ecosystem, a successor and several similar devices are still being developed [1, 20]. While for the wearer of such devices recording and sharing of images and videos gets easier, many bystanders perceive these devices as disruptive and fear substantial negative consequences on their digital privacy because of non-consensual sharing of graphical material which contains them [5, 17]. This highlights the need for effective tools to preserve and mediate our digital privacy.

There is still a distinct lack of privacy tools to enable users to restrict what others may share about them. This is even true for benevolent scenarios in which the recording party is willing to respect the privacy wishes of bystanders. The ubiquity of recording devices makes getting informed consent of all bystanders unfeasible and new technologies and concepts are needed to enable users to express their privacy wishes in such a way that others can respect them. We believe this is one of the major privacy challenges in the face of the proliferation of wearable cameras which can take pictures and videos at almost any time or place. Denning et al. [4] presented a study on individuals' reactions when they are bystanders around lifelogging devices with first-person cameras. There also have been numerous suggestions for countermeasures that suffer from severe limitations in practice [11, 12].

In this paper we focus on one particularly interesting scenario which has not received much attention to date, namely how privacy preferences can be communicated in situations where people are constrained in what they can carry or wear, for instance at the beach or while sunbathing. Inspired by the literature on privacy challenges concerning wearables, we investigated potential countermeasures to protect the privacy of bystanders in this scenario and contrast it to a traditional scenario, such as sitting in a cafe. In particular we investigated whether users would be interested in and accept wearable PETs to counter privacy threats in public spaces.

We conducted qualitative interviews to study the perceptions about three different PETs that could be used to communicate privacy preferences to recording devices and/or sharing services. We designed the three abstract PETs based on related work to cover a broad spectrum of possibilities.

To evaluate users' attitudes towards our approaches, we conducted 20 semi-structured interviews at a local beach, where we approached people wearing bathing wear and in a local cafe. Our goal on the one hand was to gain an understanding of users' privacy concerns towards wearable cameras such as Google Glass, and on the other hand which kind of PET they would like to use to preserve their privacy. We were particularly interested in whether the location of the interviews would influence the participants' perceptions and preferences. Our hypothesis was that in the beach environment the clothing-based PET would be the preferred option, while in the cafe environment there would be a mix of preferences. Our findings show that most of our participants had serious concerns regarding their privacy when confronted with Google Glass. Furthermore, and to our surprise, we found that the privacy-bracelet was the preferred PET for most of our participants, irrespective of location.

The primary contribution of our work is a comparative study of three meta-PETs across two very different locations. While most related work discusses attitudes in general or specific to one PET, to the best of our knowledge this is the first work to study attitudes towards different categories of PETs in relation to different locations.

USEC '17, 26 February 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2017.23001

II. Related Work

Various methods have been proposed to allow individuals to defend their privacy against non-consensual disclosure of pictures and videos. As concealing one's face (e.g. with a mask) is not socially or legally accepted everywhere, several methods have been proposed to communicate picture privacy preferences towards cameras. The respectful cameras approach as presented in [18] uses hats and scarfs as visual markers. The picture privacy policy framework presented in [3] uses a similar approach. Contrary to [18], the picture privacy policy framework uses not only accessories but also T-shirts to encode privacy policies. The used encoding scheme is designed in an unobtrusive way with almost no impact on apparel appearance. FaceBlock [21] uses biometric features as visual markers instead of wearable artifacts.

As most portable devices come with GPS sensors, location-based technologies such as the SnapMe privacy watchdog [7] or Blind Spot [13] are feasible to mediate privacy preferences. In comparison to SnapMe, the Blind Spot approach is based on fixed cameras and intended for CCTV-like surveillance systems. Halderman et al. [6] presented a location-based privacy management protocol. Barhm et al. [2] presented an approach where individuals perform gestures when recorded by a camera to be made irrecognizable. In this work, we focused on concepts that enable bystanders to control their privacy in different situations. In comparison to these concepts, PlaceAvoider [19] was designed to blacklist specific locations instead of individuals. Also, the control does not lie in the hand of the bystander. ScreenAvoider [10] was designed to protect sensitive computer screens instead of individuals. Similarily, PrivateEye [15] was proposed to protect sensitive content. WaveOff [15] could potentially be used to protect persons in public spaces. In contrary to our approaches however, the wearer of a lifelogging device controls the privacy options instead of the bystander.

The work by Hoyle et al. [8] provides insights in how wearer of a lifelogging device perceive privacy in a lifelogging context and focuses on the wearer's perspective (it also covers how wearers perceive bystander reactions) and found that people may prefer to manage privacy through in situ, physical control of image collections. Roesner et al.'s [16] approach relies on a centralized authority and compared to our approaches allows to specify policies for users and objects irrespective of context.

III. Wearable Privacy Enhancing Technologies

At the time of writing, there is no technical solution available on the market to communicate privacy preferences towards wearable cameras. In scholarly articles, very little attention has been paid to the challenge of designing usable technologies to tackle this issue. In this section, we present three abstract PETs to study users perceptions and attitudes towards these different methods. They have been assembled based on existing approaches and related work as presented above. For the purpose of this study, we presented best-case working scenarios, since we were mainly interested in the attitudes and perceptions of the users to the potential of the concepts. Therefore, we left out many of the technical challenges which still need to be overcome. As shown in previous work, privacy preferences are highly context-dependent [8, 9, 14].

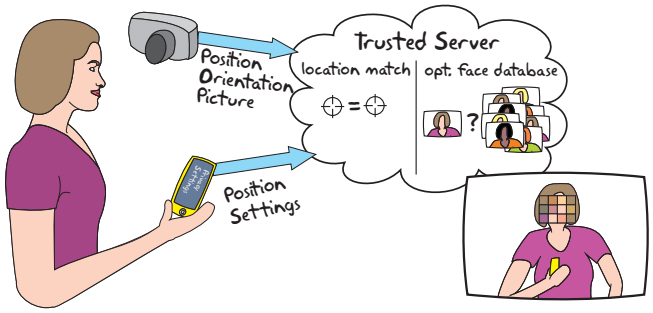

Fig. 1. For illustration to the reader only: The translated diagram explaining the Privacy App concept

A. The Privacy App

The *Privacy App* is mainly inspired by the SnapMe [7] and FaceBlock [21] apps. Both apps have a range of configuration options. For the purpose of this study, we defined that the location of the app user and the location of the nearby cameras are transmitted to a photo sharing server together with the privacy preferences of the user. Due to the co-location information the photo sharing service can blur the faces of people with corresponding app configurations when a photo is uploaded. This feature is additionally supported by face recognition software. This concept represents the traditional technology approach.

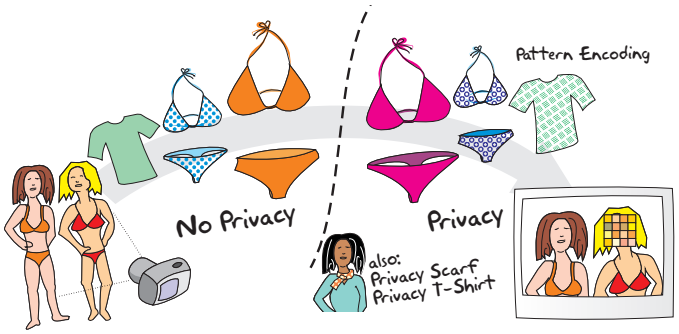

Fig. 2. For illustration to the reader only: The translated diagram explaining the Privacy Fabric concept

B. The Privacy Fabric

The *Privacy Fabric* is a piece of cloth to communicate a user-defined privacy policy. The concept is inspired by P3F [3] and privacy hats and scarfs by Schiff et al. [18]. It is based on pattern recognition and works without additional hardware. To create a privacy cloth, e.g., swimming trunks, T-shirts or any other piece of clothing with a privacy pattern, clothing and accessory manufacturers can use a specific encoder to create a visual marking or pattern that matches any wardrobe style. Either the wearable doing the recording or the photo sharing service can detect if a person is wearing a piece of clothing with a privacy preference encoded in it and can blur those peoples' faces. The main advantage of this method is that it is unobtrusive as no piece of technology needs to be operated. This concept represents the most *wearable* PET and we hypothesized that users would prefer this in the beach

scenario since it would allow them to express their privacy preferences in an unobtrusive way.

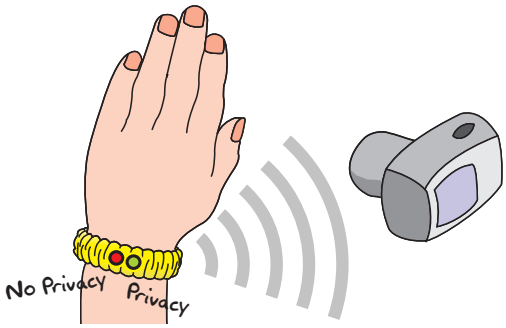

Fig. 3. For illustration to the reader only: The translated diagram explaining the Privacy Bracelet concept

C. The Privacy Bracelet

We designed the concept of the *Privacy Bracelet* as a mix between the privacy smartphone app and the privacy fabric. While it uses technology of similar power to the smartphone, it is wearable, similar to fitness trackers (e.g., FitBit). This concept was not based on related work but was designed to give us a half-way point between the two PETs described above and allow us to have middle ground during the interviews to be able to contrast between the two technologies described above. In our concept the privacy bracelet has a simple button to turn privacy on and off. If the privacy button is turned on, the device emits a signal that wearable cameras would be able to detect and blur the faces of the bracelet wearers.

IV. User Study

A. Methodology

The aim of this study is to evaluate users' attitudes toward wearables in the two scenarios (beach and cafe) and the PETs concepts presented above. We conducted field sessions with semi-structured interviews at a public beach and in a cafe. 20 participants were recruited. The participants were compensated for their time with ice cream. During the field sessions, two researchers were present.

The interview sessions proceeded as follows: the two researchers approached potential users of the proposed PETs, i.e. groups of bathers wearing bikinis or swimming trunks and people in a cafe. Furthermore, the participants could use Glass with the video and picture capabilities enabled to gather hands on experience. The interview consisted of two parts: In the first part, we examined privacy concerns related to Glass. The second part focused on the proposed artifacts to express privacy preferences. After a brief introduction to the purpose of the study, the interviews began with questions on Google Glass and privacy. Afterwards, the researchers presented the three PETs as described above. The three methods were described using illustrations in a neutral way without any hints on who developed the method. To preserve the participants' privacy during the recruitment and the interview sessions, all recording functions of Glass were disabled. We recorded the interview sessions (audio only) after the participants gave their consent. Additionally, one of the researchers took notes during and after the interview sessions. The only personal information we collected were age, gender and profession. The interview questions can be found in the Appendix VIII.

B. Coding

After the data collection, we went through the interviews and produced an initial set of codes. To do so, we traversed the data segments from the interview to each question. Two researchers performed the initial coding independently of each other to minimize the susceptibility of biased interpretation. After the initial coding process, we discussed the retrieved codes, recurring themes, patterns and connections. Additionally, we compared the codes with the ones presented in [4]. After agreeing on a set of codes, we used the codebook for a final coding of the interview data. All interview segments were coded, regardless if they emerged directly from a question or a subsequent discussion.

V. Results

In this section, we present the results of our user study. As our evaluation is based on qualitative data, we place the emphasis on an exploration of the ideas and insights of the participants instead of a quantitative analysis. However, some of the numbers are given as a rough indicator of trends which we spotted during the study. These will however need to be backed up by a larger quantitative study.
In total, we interviewed 20 participants. They were recruited at a public beach and in a cafe. 9 participants were male and 11 were female, and the age ranged between 19 and 42 (median age: 25). After 20 participants, we reached saturation and little to no further insights were gained, so we concluded the study.

Technology Familiarity

All of the participants had at least a rough idea of Google Glass and its basic functionality. They were all aware of Glass' ability to record pictures and videos. Most of them (17/20) immediately associated a camera with the device when they saw us passing by with it.
We collected information on profession and highest level of education. None of our participants was working in an IT-related field. 10 had completed high-school, 4 had a bachelor degree, 2 a master degree and 4 did not complete high-school. To tie our results to existing literature, we based questions on privacy on those from Denning et al.[4].

Privacy Considerations

About 12 participants expressed discomfort and irritation as bystanders of Glass-like devices. They were concerned about their privacy and perceived that they lose control over their images and videos. About half of the participants found it disturbing that they cannot see if the Glass-wearer in front of them actually records a video or not. Six participants even expressed vexation and had serious concerns regarding mass surveillance.

> *"If someone wore it [Google Glass] in front of me, I'd definitely ask him to take it off."*
> P13 (25, male)

"I have the feeling that [with Google Glass] something serious is going on concerning surveillance. Maybe Glass performs face recognition in the background and transmits the information about the recorded people to the NSA. This would make every Glass-wearer an unintended little helper of the NSA."
P19 (42, male)

In contrast, 8 (younger) participants reported a neutral feeling towards augmented reality devices and continuous recording. Most of them said that, over time, they have gotten used to it and perceive the numerous cameras they are surrounded with as a part of their everyday lives. Remarkably, they did not distinguish between governmental surveillance, CCTV or consumer devices such as smartphones and wearables. One third of the participants said that their privacy concerns vary depending on the context.

PETs Preferences

In general, all participants expressed a strong interest in a privacy enhancing or mediating technology to communicate their privacy preferences towards Glass users. On average, our participants indicated an interest of 4.3 on a 5-point Likert scale, where 1 means no or little interest and 5 means high interest. The lowest indicated number was 3. After presenting the three methods (as described above), 13 participants preferred the privacy bracelet. 4 preferred the app and only 2 the privacy fabric. One participant said that he finds all of the suggested methods useless. We saw no trend difference between participants preferences based on the location we conducted the interview in. We found these results somewhat surprising. We had expected a trend towards favoring the privacy fabric in the beach environment and more of a mix or potentially a trend towards the more traditional smartphone app in the cafe scenario. The main reason for the preference as indicated by the interviewees was ease of use and convenience. Many who supported the bracelet said that they found the user interface very intuitive. Some also favored the anonymous aspect of how the data is transmitted to the camera. Many participants mentioned that they do not want facial recognition and location tracking, as performed by the privacy app in the background. They perceived the use of such methods in privacy tools as paradoxical.

"The server behind the app bothers me just as much as Google Glass does."
P15 (24 years, male)

Thirteen interviewees favored the privacy bracelet because it does not exclude social network deniers or people without a smartphone. Eight participants also liked the idea behind the privacy fabric but mentioned concerns with respect to personal styling preferences and mentioned it could be complicated to adjust their clothing based on their context-related privacy preferences.

Privacy & Context

As previously stated, one third of our participants indicated that their privacy concerns vary depending on the context. They mentioned parties with alcohol and their own home as privacy-sensitive spaces. Concerning PETs however, 16 participants said that they made their choice independently from the location of use. They said that such a tool should work regardless of the environment. We observed no qualitative difference in the responses between the groups we interviewed at the beach and the cafe.

"In general, I don't really care about privacy. But I would not want to be filmed drinking during a party."
P17 (19, female)

Price

Concerning the price people thought the PETs should cost, the suggestions varied greatly. For the privacy bracelet, the lowest suggested price was 10 euros. Three participants said that they would be willing to pay about 150-200 euros. They explained their suggestions based on how highly they value privacy. Many participants said that such a device should not be too expensive so that anyone could afford it. For the app, the highest nominated price was 2 euros. Assuming that the price for a privacy fabric and an ordinary one would be the same, most participants reported that they would buy the privacy fabric due to its additional functionality.

VI. Discussion

Our results have shown that potential users of PETs want an easy-to-use user interface. For many of them, pushing a button instead of wearing dedicated artifacts is more intuitive and gives them a sense of control. Our results suggest that more and more people desire solutions that work independently of other systems such as smartphones, social networks and other online services that require registration.

To our surprise, our participants showed little trust in the privacy-fabric. The concept was hard to understand and imagine for most of our participants. Therefore, they showed little trust in this method in comparison to the privacy bracelet. This has significant implications for our research, since we had thought this was a very promising novel PET. We also found that the preference for a certain meta-PET did not depend on the location of the interview.

Our results indicate that many users prefer technologies that do not require facial recognition, location tracking and the transmission of sensitive information to (trusted) servers as they perceive this as a violation of their privacy. Furthermore, we found that the preference of a certain PET does not depend on the location. These results pose some serious challenges for the development of future PETs to help mediate privacy preferences in the age of wearable computing.

We chose the two scenarios because we felt they offered good extremes to begin researching the question of how different classes of PETs are perceived in different scenarios. Again since this is a Note we did not want to cover the entire design space but offer insights into specific scenarios that can serve as a starting and calibration point for more broad work. Also, we chose the beach scenario as we wanted to cover a situation in which participants are potentially constrained in what technical artefacts they can carry or wear. The beach is a challenging environment for PETs and to the best of our knowledge has not been studied in relation to PETs yet. We also expected the beach to elicit stronger privacy concern. We find it an interesting result that this did not seem to be the case for our participants. While many other environments are interesting

and worth studying we think these two offered a good start and useful insights.

During the interviews, some participants wanted to wear Google Glass and play around with it. To explore its functionality, they had to turn it on and some of them took pictures and videos. After we continued with the interviews, we again disabled all the recording functions. We observed that during the time the participants wore it, most of their concerns vanished but immediately returned when they gave it back to us.

VII. Limitations

For our interviews, we deployed Google Glass in a public space to confront potential participants with this new technology and to provoke the privacy concerns implied by its presence. As described above, we systematically recruited participants who showed reactions towards Glass for our interviews. Amongst them, most individuals who were 30 or younger immediately agreed to give an interview and showed high interest in this topic. In contrast, many people over 30 refused to talk to us and expressed annoyance and irritation. Since it was significantly harder to recruit participants over the age of 30, and all interviews were conducted in an urban area, the results will probably differ for other demographics. Also, as we conducted semi-structured interviews, we collected self-reported data and as a consequence, our results are based on subjective views and perceptions.

VIII. Conclusion

In this paper, we presented three different abstract PETs to enhance the privacy of individuals in relation to Google Glass or similar wearables. In 20 semi-structured interviews conducted at a public beach and in a cafe, we examined people's privacy considerations related to Google Glass-wearers in their surrounding. We found that many people have serious concerns regarding potential privacy violations and that there is high demand for usable PETs. In the course of our interviews, we presented three abstract PETs and asked the participants about their preferences concerning them. Most participants preferred the privacy bracelet, a wearable artifact with an intuitive user interface that does not transmit sensitive information to third parties. We saw no differences based on the location of the interview. Furthermore, we determined that people prefer a solution that does not exclude particular user groups such as smartphone and social network abstainers. These results pose significant challenges to future PETs designs since many features our participants found critical are currently used in PETs found in related work. We also found the lack of support for wearable PETs such as the privacy fabric surprising, and we plan further studies to discover more details on why this is the case and whether the concept can be adapted to make it more acceptable.

Acknowledgment

The research was partially funded by COMET K1, FFG - Austrian Research Promotion Agency - and by the *netidee* grant program from the Internet Foundation Austria (IPA).

References

[1] Ars Technica. *Google Glass now "Project Aura", ex-Amazon Fire Phone employees hired*. http://arstechnica.com / gadgets / 2015 / 09 / google - glass - now - project - aura-ex-amazon-fire/phone-employees-hired/, accessed 9/13/2015. 2015.

[2] Mukhtaj S Barhm et al. "Negotiating privacy preferences in video surveillance systems". In: *Modern Approaches in Applied Intelligence*. Springer, 2011, pp. 511–521.

[3] Adrian Dabrowski, Edgar R Weippl, and Isao Echizen. "Framework Based on Privacy Policy Hiding for Preventing Unauthorized Face Image Processing". In: *Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on*. IEEE. 2013, pp. 455–461.

[4] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. "In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies". In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM. 2014, pp. 2377–2386.

[5] Serge Egelman. *When Everyone's A Cyborg: Privacy and Security in The Age of Wearable Computing*. Keynote by Serge Egelman at the Workshop on Usable Security (USEC'14). 2014.

[6] J Alex Halderman, Brent Waters, and Edward W Felten. "Privacy management for portable recording devices". In: *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*. ACM. 2004, pp. 16–24.

[7] Benjamin Henne, Christian Szongott, and Matthew Smith. "SnapMe if you can: privacy threats of other peoples' geo-tagged media and what we can do about it". In: *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM. 2013, pp. 95–106.

[8] Roberto Hoyle et al. "Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras". In: *Proceedings of The ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '15)*. Apr. 2015, pp. 1645–1648. DOI: 10.1145/2702123.2702183.

[9] Giovanni Iachello and Jason Hong. "End-user privacy in human-computer interaction". In: *Foundations and Trends in Human-Computer Interaction* 1.1 (2007), pp. 1–137.

[10] Mohammed Korayem et al. "Screenavoider: Protecting computer screens from ubiquitous cameras". In: *arXiv preprint arXiv:1412.0008* (2014).

[11] Katharina Krombholz et al. "Ok Glass, Leave me Alone: Towards a Systematization of Privacy Enhancing Technologies for Wearable Computing". In: *WEARABLE'15 Workshop at Financial Crypto 2015*.

[12] Karen Lamb et al. "Users? Privacy Perceptions About Wearable Technology: Examining Influence of Personality, Trust, and Usability". In: *Advances in Human Factors in Cybersecurity*. Springer, 2016, pp. 55–68.

[13] Shwetak N Patel, Jay W Summet, and Khai N Truong. "Blindspot: Creating capture-resistant spaces". In: *Protecting Privacy in Video Surveillance*. Springer, 2009, pp. 185–201.

[14] Sameer Patil et al. "Reasons, rewards, regrets: privacy considerations in location sharing as an interactive

practice". In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM. 2012, p. 5.

[15] Nisarg Raval et al. "Markit: Privacy markers for protecting visual secrets". In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. ACM. 2014, pp. 1289–1295.

[16] Franziska Roesner et al. "World-driven access control for continuous sensing". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2014, pp. 1169–1181.

[17] Florian Schaub et al. "A Design Space for Effective Privacy Notices". In: *SOUPS '15*. 2015.

[18] Jeremy Schiff et al. "Respectful cameras: Detecting visual markers in real-time to address privacy concerns". In: *Protecting Privacy in Video Surveillance*. Springer, 2009, pp. 65–89.

[19] Robert Templeman et al. "PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces." In: *NDSS*. 2014.

[20] The Wallstreet Journal. *Google Isn't Giving Up on Glass, Eric Schmidt Says*. http://blogs.wsj.com/digits/2015/03/23/google-isnt-giving-up-on-glass-schmidt-says/, accessed 9/9/2015. 2015.

[21] Roberto Yus et al. "Demo: FaceBlock: privacy-aware pictures for google glass". In: *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*. ACM. 2014, pp. 366–366.

APPENDIX

Interview Questions

1) Do you know what this is?
2) Did you know that you can record video with those kinds of glasses?
3) How do you feel about being around someone who is wearing those kinds of glasses?
4) Do you have any privacy concerns?
5) On a scale from 1-5, how much would you be interested in a technology or product to protect your privacy?
6) Would you want someone to ask for permission before recording a video?
7) Would you want to be asked for permission before being recorded?
8) Which of the proposed methods would you prefer? 5 point Likert scale?
9) Why would you prefer this method?
10) Imagine you are in a cafe/at the beach instead of in this cafe/at this beach, which method would you prefer and why?
11) Back at the cafe/beach, would you still prefer this method?
12) How much would you pay for the presented techniques to express your privacy preference?
13) Would you buy additional clothing or accessories such as bikinis, t-shirts, scarves?
14) How much would you pay for such an app?
15) How much would you pay for such an electronic device?