10-10-2020

A User Study of a Wearable System to Enhance Bystanders' Facial Privacy

Alfredo J. Perez

Sherali Zeadally

Scott Griffith

Luis Y. Matos Garcia

Jason A. Mouloud

IoT

MDPI

Article

A User Study of a Wearable System to Enhance Bystanders' Facial Privacy

Alfredo J. Perez [1,*], Sherali Zeadally [2], Scott Griffith [1], Luis Y. Matos Garcia [3] and Jaouad A. Mouloud [4]

[1] TSYS School of Computer Science, Columbus State University, Columbus, GA 31907, USA; griffith_scott@columbusstate.edu
[2] College of Communication and Information, University of Kentucky, Lexington, KY 40506, USA; szeadally@uky.edu
[3] Department of Electrical and Computer Engineering, Universidad Ana G. Mendez, Gurabo, PR 00777, USA; lmatos59@email.suagm.edu
[4] Department of Information Technology, Bergen Community College, Paramus, NJ 07652, USA; jmouloud@me.bergen.edu
* Correspondence: perez_alfredo@columbusstate.edu

Received: 18 August 2020; Accepted: 6 October 2020; Published: 10 October 2020

Abstract: The privacy of users and information are becoming increasingly important with the growth and pervasive use of mobile devices such as wearables, mobile phones, drones, and Internet of Things (IoT) devices. Today many of these mobile devices are equipped with cameras which enable users to take pictures and record videos anytime they need to do so. In many such cases, bystanders' privacy is not a concern, and as a result, audio and video of bystanders are often captured without their consent. We present results from a user study in which 21 participants were asked to use a wearable system called FacePET developed to enhance bystanders' facial privacy by providing a way for bystanders to protect their own privacy rather than relying on external systems for protection. While past works in the literature focused on privacy perceptions of bystanders when photographed in public/shared spaces, there has not been research with a focus on user perceptions of bystander-based wearable devices to enhance privacy. Thus, in this work, we focus on user perceptions of the FacePET device and/or similar wearables to enhance bystanders' facial privacy. In our study, we found that 16 participants would use FacePET or similar devices to enhance their facial privacy, and 17 participants agreed that if smart glasses had features to conceal users' identities, it would allow them to become more popular.

Keywords: bystanders' privacy; facial privacy; face detection; face recognition; Internet of Things; wearables; usability; usable privacy; adversarial machine learning

1. Introduction

The availability of cameras and Artificial Intelligence (AI) through wearables, mobile phones, drones, and Internet of Things (IoT) devices is making bystanders' facial privacy more significant to the general public. Bystanders' privacy arises when a device that collects sensor data (such as photos, sound or video) can be used to identify third-parties (or their actions) when they have not given consent to be part of the collection [1,2]. Even though bystanders' privacy has been an issue since the end of the 19th century with the invention of portable cameras that could take photos in a short amount of time [1], recent advances of camera-enabled devices (e.g., mobile phones, IoT) combined with Artificial Intelligence (AI) and the Internet have raised awareness about this privacy issue especially in the last couple of years. We show in Figure 1 some of issues related to bystanders' facial privacy.

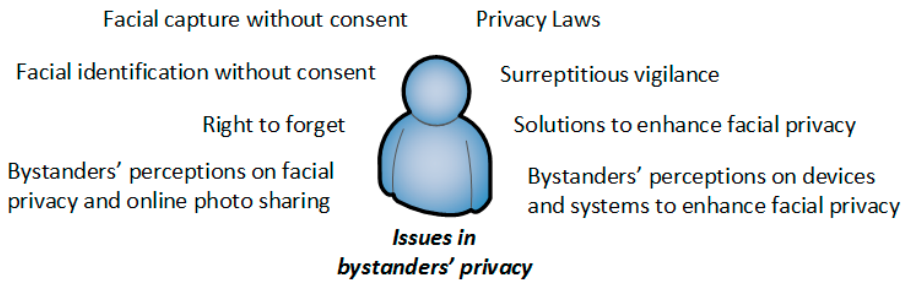


Figure 1. Issues related to bystanders' privacy. Our focus in this work is to study bystanders' perceptions of a bystander-centric device/system to enhance facial privacy.

Recently, various solutions [3–24] that address bystanders' privacy have been proposed in the literature. However, most of these solutions rely on bystanders trusting third-party devices or systems which do not give a choice to protect their privacy. To enable bystanders to protect their privacy, we have developed the Facial Privacy Enhancing Technology (FacePET) [25] smart wearable device. FacePET is a wearable system made of intelligent goggles worn by bystanders to protect their privacy from unauthorized face detection. FacePET operates on image features (in particular Haar-like features [26]) through visible light produced by the FacePET goggles to confuse face detection algorithms based on the Viola–Jones face detection algorithm [27]. If an unauthorized party takes a photo of the bystander with the FacePET system enabled, the action on the features is registered in the photo. Thus, if later an Artificial Intelligence (AI) algorithm based on the Viola–Jones algorithm attempts to detect a bystander's face, the goal of the FacePET is to prevent detection of the bystander's facial features by the AI algorithm.

The FacePET goggles are controlled via a mobile application at the bystanders' mobile phone which permits the bystander to create privacy policies to automatically provide consent to third-party cameras. When a third-party authorized by the bystander wants to take a photo of the bystander, FacePET turns off the goggles and disables the operation.

The concept of consent is a cornerstone in privacy [28–30], and in this context, FacePET improves upon previous bystander-based approaches to protect facial privacy by allowing the bystander to create his/her own privacy policies and provide the consent. We describe the complete FacePET system, how it acts on Haar-like features based on the Viola–Jones face detection algorithm, and its effectiveness in [25].

In this work, we present the results of a small user study with a focus on perceptions of users about the FacePET system and intelligent goggles with features to mitigate facial detection algorithms. While there have been past works [8,14,31–40] on understanding the perceptions of bystanders with respect to facial privacy, to the best of our knowledge, our user study is the first to address the perceptions of a smart wearable (IoT) system worn by bystanders with a privacy protection focus.

Research contributions of this work

We summarize the main research contributions of this work as follows:

- We present a summary of human–computer interaction studies and systems related to facial privacy.
- We present a user study of the FacePET system with a focus on users' perceptions about the device and intelligent goggles with features to mitigate facial detection algorithms.
- We discuss the results of the study to further enhance the FacePET system, as well as influence the development of future bystander-centric devices for facial privacy.

The rest of this paper is organized as follows. Section 2 presents a review of related works. In Section 3 we describe the FacePET system. Section 4 presents the results of our usability evaluation of FacePET. Finally, in Section 5, we make some concluding remarks and present future work.

2. Related Works

2.1. Bystanders' Facial Privacy: Human–Computer Interaction (HCI) Perspective

From the HCI perspective, research studies related to bystanders' privacy can be classified into two groups: (1) understanding the utilization/adoption of mobile, camera-enabled devices (i.e., mobile phones, wearables, IoT, and drones), and related technologies in shared spaces; (2) usability studies for facial privacy systems. These studies have been conducted using a variety of methods such as interviews, analysis of logged data (i.e., voice-mail diaries), online web comments, surveys, and a combination of more than one of these methods. We highlight some of these studies in Table 1.

Table 1. Human–Computer Interaction (HCI) studies related to Bystanders' Facial Privacy.

Reference	Research Focus	Approach	Comments
Palen et al. [31]	Mobile phones in shared spaces	19 new mobile phone users tracked for six weeks. Voice mail diaries, interviews and calling behavior data collected for four months	Users were inclined to modify their perceptions on social appropriateness from initial use. Highlighted a conflict of spaces (physical vs. virtual)
Denning et al. [32]	Augmented Reality (AR) glasses	12 field sessions with 31 bystanders interviewed and their reactions to a co-located AR device	Participants identified different factors on making recording more/less acceptable and they expressed interest on being asked for consent to be recorded and record-blocking devices
Motti et al. [33]	Wearable devices including armbands, smart watches, earpieces, head bands, headphones and smart glasses	Observational study of online comments posted by wearable users. A total of 72 privacy comments analyzed	Identified 13 user's concerns about wearable privacy related to the type of data and how device collects, stores, processes and shares data. Concerns depend on type and design of device
Hoyle et al. [34]	Lifelogging with wearable camera devices	In situ user study in which 36 participants wore a lifelogging device for a week, answered questionnaires on photos captured, and participated in an exit interview	Users preferred to manage privacy through in situ physical control of image collection (rather than later), context determines sensitivity, and users were concerned about bystanders' privacy although almost no opposition or concerns were expressed by bystanders during study
Hoyle et al. [35]	Privacy perceptions of online photos	Survey deployed through Amazon Mechanical Turk (mTurk) with 279 respondents. Survey used 60 photos showing 10 different contextual conditions	Respondents shared common expectations on the privacy norms of online images. Norms are socially contingent and multidimensional. Social contexts and sharing can affect social meaning of privacy
Zhang et al. [36]	Privacy attitudes on video analytics technologies	10 day longitudinal in situ study involving 123 participants and 2328 deployment scenarios	Privacy preferences vary with a number of factors (context). Some contexts make people feel uncomfortable. People have little awareness on the contexts where video analytics can be deployed
Hatuka et al. [37]	Smartphone users' perceptions about contemporary meaning of public/private spaces	Correlational study with 138 participants who took surveys and were observed by researchers for three months. Participants divided in two groups: basic phone users and advanced smart phone users	Differences on the meaning of public/private spaces may be blurred and may be dynamically redefined by use of technology

Table 1. *Cont.*

Reference	Research Focus	Approach	Comments
Wang et al. [38]	Civilian use of drones/Unmanned Aerial Vehicles (UAVs)	16 semi-structured interviews to examine people's perceptions on drones and usage under five specific scenarios. Participants were shown a real drone and videos about its capabilities before interview	Differences on the meaning of public/private spaces for participants. Participants highlighted inconspicuous recording and inaccessible drone pilots to request for privacy as concerns and some participants expected for expected for consent to be asked before recording by drones
Chang et al. [39]	Drones	Laboratory study with 20 participants using real and simulated drones to elicit user perceptions about drone security and privacy. Study also used surveys, interviews and drone piloting exercises	Drone design affects privacy and raises security concerns with drones. Recommended the use of geo-fencing to address privacy concerns, designated fly-zones/"highways" for drones. Auditive and wind clues to inform of drone usage for bystanders
Steil at al. [8]	User evaluation of a privacy-preserving device to block a head-mount camera	12 participants with semi-structured one-to-one interviews to evaluate an eye gesture-activated first-person camera shutter blocker device controlled by Artificial Intelligence (AI) 17 participants annotated video datasets for training data	Eye-tracking can be used as a way to handle bystanders' privacy as camera activates when person fixes eyesight. Non-invasive on the user. Eye tracking not perceived in general as a threat to privacy by participants. Privacy sensitivity varies largely among people, thus affecting the definition of privacy
Aditya et al. [14]	Personal expectations and desires for privacy on photos when photographed as a bystander	Survey deployed online via Google Forms with 227 respondents from 32 different countries	Privacy concerns and privacy actions varied based on context (i.e., location, social situations)
Ahmad et al. [40]	People's perceptions of and behaviors around current IoT devices as bystanders	Interview study with 19 participants	Participants expressed concerns about uncertainty of IoT device's state (if they were recording or not) and their purpose when being bystanders around these devices
Our approach (FacePET)	User study of a bystander-based wearable (smart glasses) to attack facial detection algorithms	21 participants took survey on bystanders' privacy, wore the FacePET device, saw the results of facial privacy protection on their faces, and answered questions on the usability of FacePET	Most participants would use FacePET or a bystander-based facial privacy device. Most participants agreed that facial privacy features would improve the use and adoption of smart glasses

We describe below some of the common findings among these studies:

- Seven studies in Table 1 recruited less than 36 participants (five studies recruited 20 or less participants [8,31,38–40], and two studies recruited less than 36 participants [32,34]. Only two studies recruited more than 100 participants [36,37]. The studies with less than 36 participants use interviews, observation, testing of devices and some of them use surveys. The studies with more than 100 participants use surveys or automated ways (AI) to gather data of interest.
- The definitions of private/public (shared) spaces and privacy perceptions vary among individuals. What is meant for a private/public space seems to depend on context (i.e., individuals, actions and devices used at any given location).
- The design of the data capturing device has an impact on user and bystanders' privacy perceptions.
- Individuals want to have control of their facial privacy even though some contexts are less private-sensitive than others.

In contrast to the related works discussed above which focused primarily on privacy perceptions of users/bystanders when photographed in shared/public spaces by different kinds of devices, and their perceptions about how these photographs are shared in social networks and used by external parties (i.e., in web/remote services for facial recognition), in this work we explore the perceptions of a bystander-centric device (smart goggles) to protect bystanders' facial privacy. To the best of our knowledge, our study is the first study to explore user perceptions of a bystander-centric IoT/wearable system with a focus on privacy.

2.2. Bystanders' Facial Privacy: Solutions

In the past we proposed a taxonomy [1] to classify solutions to handle bystanders' facial privacy. Our taxonomy is composed of two major groups of solutions: location-dependent methods and obfuscation-dependent methods. Methods in these categories have differences in terms of effectiveness [25], usability [41], and power consumption [42]. We show this taxonomy in Figure 2 and we present a summary of methods under each category in Table 2.

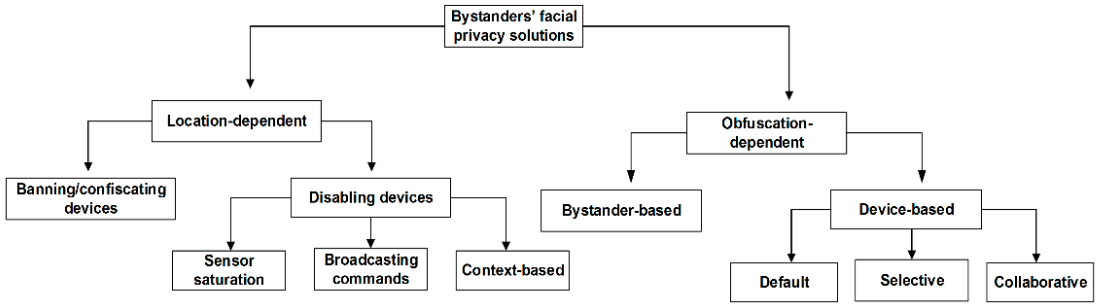


Figure 2. Taxonomy of methods for bystanders' privacy protection [1].

Table 2. Recently proposed technological solutions for bystanders' facial privacy.

Category	Subcategory	Method
Location *Methods disable or ban the utilization of capturing devices*	Disabling devices–sensor saturation	BlindSpot [3]
	Disabling services–Broadcasting of commands	Using infrared to disable devices [4]
		Using Bluetooth to disable devices [5]
	Disabling devices–context-based	Virtual Walls [6]
		Privacy-restricted areas [7]
		World-driven access control [15]
		Sensor Tricorder [16]
		PlaceAvoider [17]
		PrivacEye: [8]
Obfuscation *Methods hide the identity of bystanders' faces to avoid identification*	Bystander–based	NotiSense [9]
		PrivacyVisor [10]
		PrivacyVisor III [11]
		Perturbed eyeglass frames [12]
		Invisibility Glasses [18]
	Device-based–default	Privacy Google StreetView [19]
	Device-based–selective	ObscuraCam [13]
		Respectful cameras [21]
		Invisible Light Beacons [23]
		Negative face blurring [24]
	Device-based–collaborative	I–pic [14]
		PrivacyCamera [20]
		Do Not Capture [22]

2.2.1. Location-Dependent Methods

The focus of location-dependent methods is to disable/enable the utilization of a capturing device at a particular location [43,44] or context. Location-based methods can be divided into two categories:

- *Banning/Confiscating devices:* Even though they are non-technological solutions, banning/confiscating devices are the oldest method to handle bystanders' privacy. In the U.S., this method was first used starting from the development of portable photographic cameras at the end of the 19th century [45]. Around this time, cameras were forbidden at some public spaces and private venues.
- *Disabling devices:* In this group the goal is to disable a capturing device to protect bystanders' privacy. Methods under this category can be further classified based on the technology used to disable the capturing device. In the first group (sensor saturation), a capturing device is disabled by some type of signal that interferes with a sensor that collects identifiable data [3]. In the broadcasting of commands group, a capturing device receives disabling messages via data communication interfaces (i.e., Wi-Fi, Bluetooth, infrared) [4,5]. In the last group (context-based approaches) the capturing device identifies contexts using badges, labels, or it recognizes contexts [46] using Artificial Intelligence (AI) methods to determine if capturing cannot take place [6–8].

2.2.2. Obfuscation-Dependent Methods

The goal of obfuscation-dependent methods is to hide the identity of bystanders to avoid their identification. Depending on who performs the action to hide a bystander, these methods can be classified into two categories:

- *Bystander-based obfuscation:* In this category, bystanders avoid their facial identification either by using technological solutions to hide or perturb bystanders' identifiable features, or by performing a physical action such as asking somebody to stop capturing data, or simply leaving a shared/public space. Our FacePET [25] wearable device falls into this category.
- *Device-based obfuscation:* In this group, third-party devices which are not owned by the bystander perform blurring or add noise (in the signal processing sense) to the image captured from the bystander to hide his/her identity. Depending on how the software at the capturing device performs the blurring, solutions in this category can be further classified into default obfuscation (any face in the image will be blurred) [19], selective obfuscation (third-party device users select who to obfuscate in the image) [20], or collaborative obfuscation (third-party and bystander's device collaborate via wireless protocols [47] to allow a face to be blurred) [21]. A drawback of device-based obfuscation method is that a bystander must trust a device that he/she does not control to protect his/her privacy.

3. The FacePET System

3.1. Adversarial Machine Learning Attacks on the Viola–Jones Algorithm

To detect a face automatically in an image, supervised machine learning (classification) methods in image processing can be used. Given an image/photo x and a face detection (classification) method/algorithm Fd, the goal of Fd is to classify (or assign a label) to the image x such that if x contains a face, then $Fd(x) = 1$, and if x does not contain a face then $Fd(x) = 0$.

The process of finding a vulnerability to make classification algorithms fail is an application of a field called adversarial machine learning [48,49] which studies how an adversary/attacker can generate attacks to render machine learning models/methods ineffective. For face detection, this process can be done by applying a transformation $Tr(x)$ on the image such that if $Fd(x) = 1$, then $Fd(Tr(x)) = 0$. In other words, if x contains a face, the goal of an adversary during the face detection process is to find a method/transformation of a face in x so the face detection method does not detect the face. The transformation can be done after the image x has been captured by a camera, which in

this case, $Tr(x)$ is performed by software, or $Tr(x)$ can be generated as part of the process to capture an image wherein a person (i.e., a bystander) in the photo has a physical method to execute the transformation which is recorded/stored in the image. Thus, the goal for FacePET is to physically generate a transformation to prevent the Haar-like features from being used by the face detection (classification) algorithm. A Haar-like feature is calculated using the following formula:

$$h(r_1, r_2) = s(r_1) - s(r_2) \quad (1)$$

In this formula, $s(r_1)$ is the average of pixel intensities in "white" regions, and $s(r_2)$ is the average of pixel intensities in the "black" regions of predefined black/white patterns that are juxtaposed over an image (or a region of an image). The patterns are engineered to train classification models using machine learning algorithms and the Haar-like features. Once the model is trained, the patterns are used in images to calculate the Haar-like features, which then serve as inputs to the trained classifier. Figure 3 presents the predefined black/white patterns used by Viola–Jones to calculate Haar-like features for face detection.

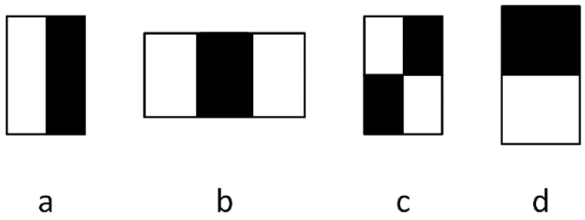
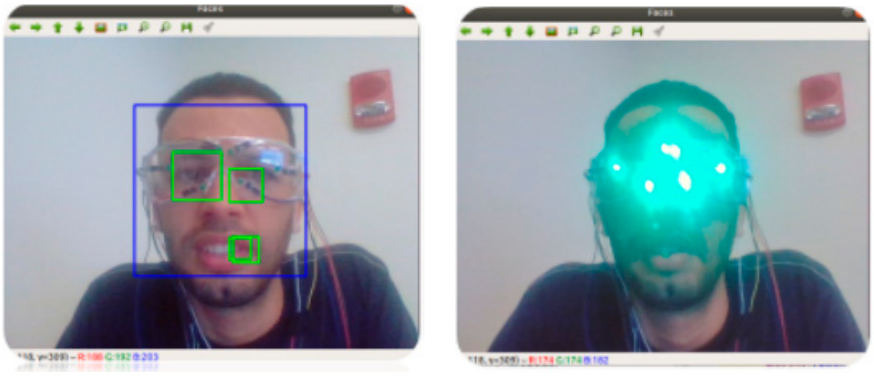


Figure 3. Predefined patterns to calculate Haar-like features in the Viola and Jones algorithm [27].

When using these patterns, the Viola–Jones algorithm creates windows of different sizes (sub-regions/sub images), calculates the Haar-like features for each window using the patterns, and then each window is passed through a classifier $Fd(x)$ that outputs 1 if a face is detected. Performing adversarial attacks on a Viola–Jones face detection algorithm can be achieved by generating noise (in the signal processing sense) in the bystander's face (or photo) such that the values of the Haar-like features make a Viola–Jones classifier fail.

In FacePET [25], PrivacyVisor [10], and Invisibility glasses [18], these attacks are performed using Light Emitting Diodes (LEDs) (either through visible light in the case of FacePET or infrared light in the case of PrivacyVisor and Invisibility glasses) embedded in goggles. Figure 4 shows an example of a detected face without the attack (Figure 4a) and an undetected face with the attack (Figure 4b). This figure shows screenshots of an application that we created using the OpenCV's implementation of the Viola–Jones algorithm to demonstrate the attack on the Haar-like features. We note that when the face is detected the software superimposes a blue square around the area of the face, and green squares around the area of the eyes and mouth (Figure 4a). However, when the features are attacked, the software fails to detect the face (Figure 4b) and no squares are superimposed on the face.



(**a**) (**b**)

Figure 4. Face detection with the Viola–Jones algorithm (**a**) Face detected/FacePET googles off; (**b**) Face not detected/FacePET with goggles on. The superposed blue and green squares in the left figure indicate the detection of a face. In the right figure, the attack with the LEDs is successful because no squares are superimposed (attack on Haar-like features performed).

Recent advances in deep learning and Convolutional Neural Networks (CNN) have improved the accuracy of image processing methods, including face detection methods. While in Viola–Jones methods the features for face detection are hand-crafted through the use patterns and Haar-like features to achieve the detection, in CNN-based algorithms there is no need for any of the two, because CNN can learn the features needed to achieve the detection through the automated training of neural networks [50]. However, CNNs for face detection can also be subject to adversarial machine learning attacks that include the optimization of adversarial generator networks for face detection [51], image-level distortions (i.e., modifications of the image's appearance not related to faces) and face-level distortions (i.e., modifications of facial landmarks in an image) [52].

3.2. The Facial Privacy Enabled Technology (FacePET) System

In Section 2.2, we described different classes of facial privacy systems that are not controlled by bystanders, and many do not provide a choice for bystanders before a photo is taken (i.e., still a bystander can be photographed inadvertently and identified without consent). These systems require bystanders to trust other parties to protect their own facial privacy without a choice or assurances to bystanders that their privacy is indeed being protected. We argue that the best types of facial privacy systems are those that provide methods for bystanders to make choices for their own facial privacy before a photo can be taken. We developed FacePET [25] under this premise. Figure 5 shows the components of the FacePET system.

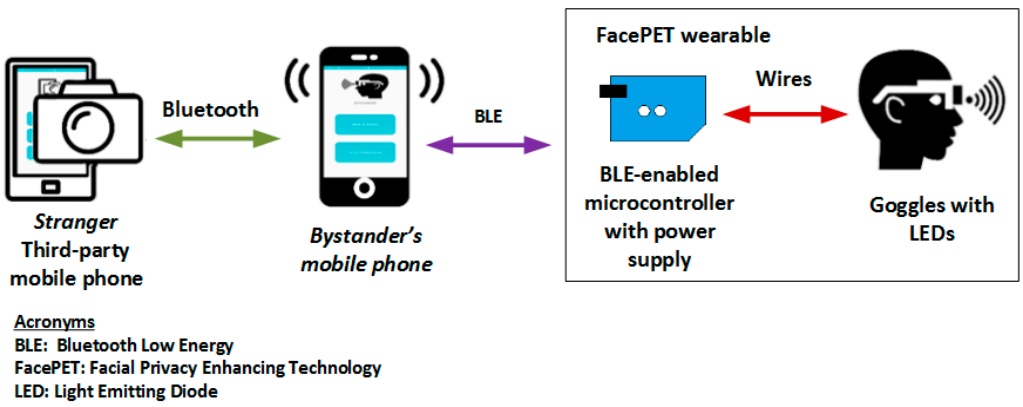
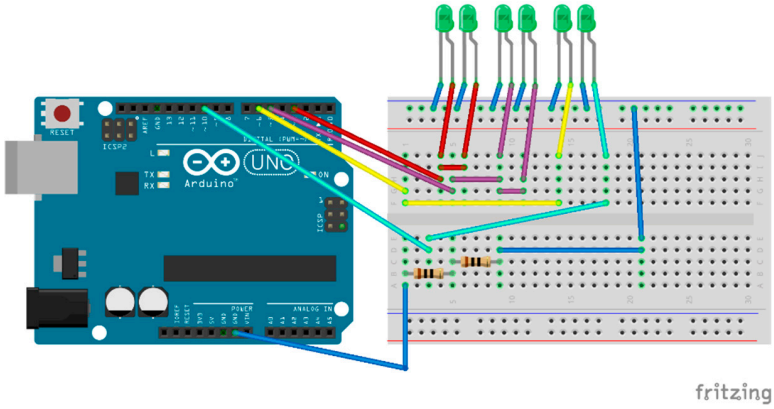


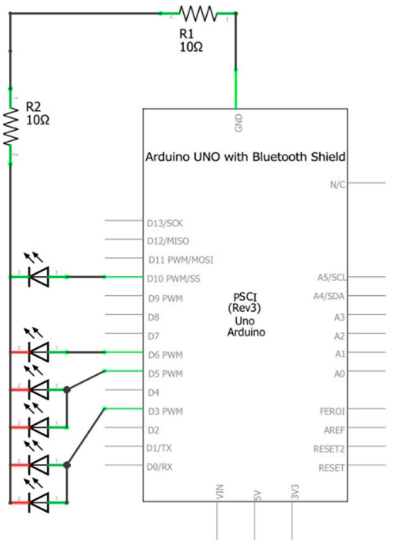
Figure 5. The FacePET system.

The major components of FacePET include:

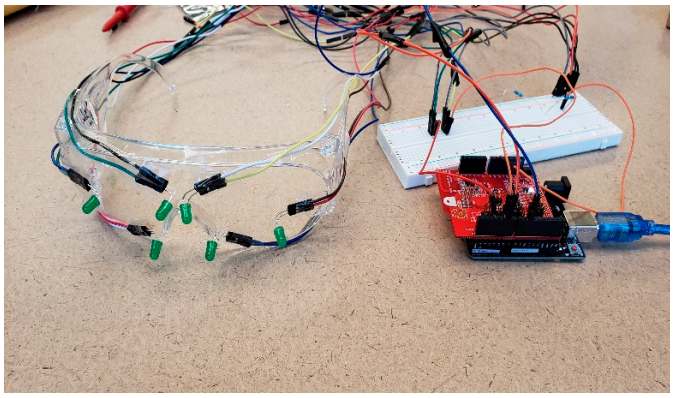
- *FacePET wearable:* The FacePET wearable (as Figure 6 shows) is composed of goggles with 6 strategically placed Light Emitting Diodes (LEDs), a Bluetooth Low Energy (BLE)-enabled microcontroller, and a power supply. When a bystander wears and activates the wearable, the FacePET wearable emits green light that generates noise (in the signal processing sense) and confuse Haar-like features for the Viola–Jones algorithm. The BLE microcontroller allows the bystander to turn on/off the lights through a Graphical User Interface (GUI) implemented as a mobile application and runs on the bystanders' mobile phone.
- *FacePET mobile applications:* We implemented two mobile applications for the FacePET system. The first mobile application, namely the *Bystander's mobile app* implements a GUI to turn on/off the FacePET wearable through commands broadcast using BLE communications. The *Bystander's mobile app* also implements an Access Control List (ACL) in which third-party cameras are authorized to disable the wearable and take photos. Different types of policies can be enforced for external parties to disable the wearable. For example, for a specific third-party user, the *Bystander's mobile app* can limit the number of times the wearable can be disabled for that third-party user. Further privacy policies based on contexts (i.e., location) can also be implemented. The second app, called the *Third-party (stranger) mobile application*, issues requests to disable the wearable and take photos of the bystander with wearable's lights off. In the current prototype, the *Third-party (stranger) mobile application* connects to the *Bystander's mobile app* via Bluetooth [53]. Figure 8 presents screenshots of both mobile applications.
- *FacePET consent protocol:* The FacePET consent protocol (as Figure 7 shows) enables a mechanism that creates a list of trusted cameras (an ACL) at the bystander's mobile application. In our current prototype the consent protocol is implemented over Bluetooth.



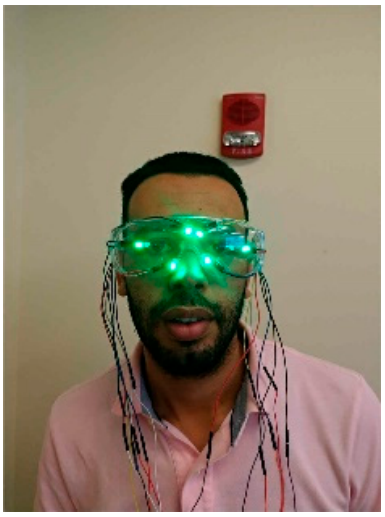
(**a**)



(**b**)



(**c**)



(**d**)

Figure 6. The FacePET wearable device. (**a**) Wiring sketch diagram for FacePET LEDs; (**b**) Schematic; (**c**) Goggles with LEDs and BLE microcontroller; (**d**) FacePET wearable prototype worn by a bystander.

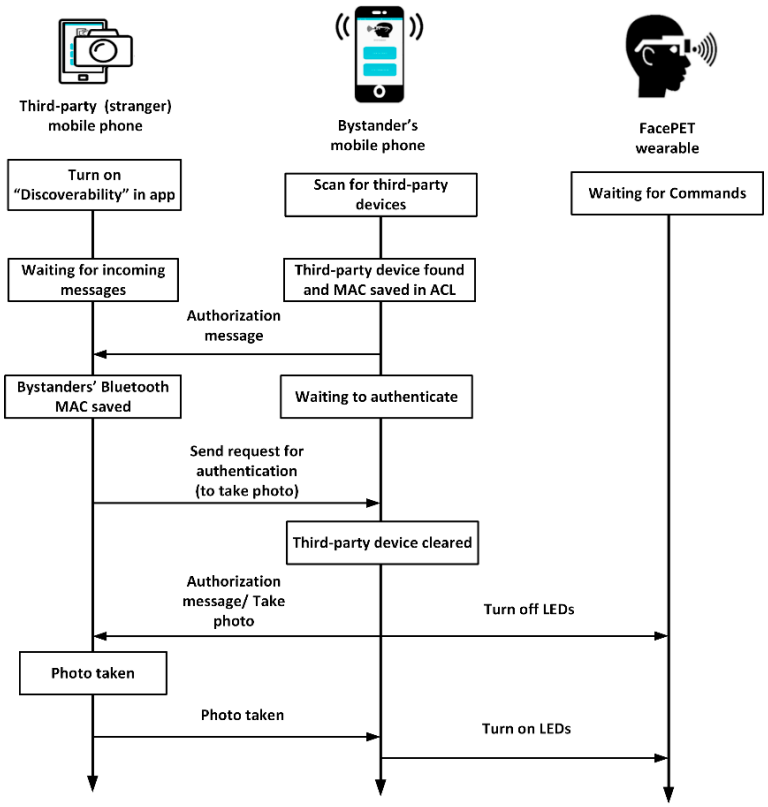


Figure 7. Sequence diagram for FacePET's consent protocol.

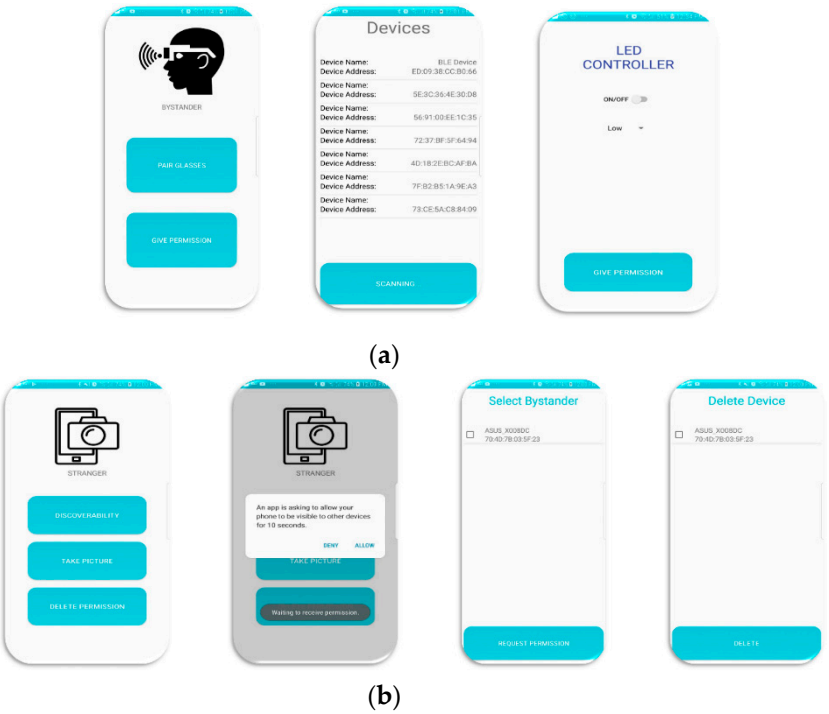


Figure 8. FacePET's system mobile app screenshots. (**a**) Bystanders' application; (**b**) Stranger (third-party).

4. A User Evaluation on Perceptions of FacePET and Bystander-Based Facial Privacy Devices

4.1. Methodology

We applied for an approval from the CSU's Institutional Review Board (IRB) to conduct our study. The initial recruitment of participants was conducted by sending a flyer through Columbus State University's (CSU) e-mail system. The flyer explained the steps for participants to take part in the study which was performed in a room at the CSU's Synovous Center for Commerce and Technology. Once in the room, each participant filled out an informed consent form that provided information about the research and its risks. Next, participants filled out an initial survey (called the "Bystander's Privacy Survey") to gauge their knowledge about the concept of bystanders' privacy as well as their personal preferences on having their photos taken in certain situations and places. We used questions from the survey developed for the I-Pic system [14]. Figure 9 shows the questions asked in the survey.

Bystanders' Privacy Survey Questions

1. Do you consider yourself a tech savvy person?
2. How often do you take pictures, videos, etc?
3. How much do you know about bystanders' privacy?
4. Do you find the issue of bystanders' privacy to be an important issue in today?
5. What would be the privacy action you would be most comfortable when at the gym?
6. What would be the privacy action you would be most comfortable when engaging in a daily outdoor activity (e.g. walking cycling, going to market places, etc.)?
7. What would be the privacy action you would be most comfortable when in a bar or a nightclub?
8. What would be the privacy action you would be most comfortable when at the beach?
9. What would be the privacy action you would be most comfortable when at your workplace?
10. What would be the privacy action you would be most comfortable when at a place of worship?
11. What would be the privacy action you would be most comfortable when at a hospital?
12. What would be the privacy action you would be most comfortable when in a restaurant?
13. What would be the privacy action you would be most comfortable when at a private gathering with family or friends?
14. What would be the privacy action you would be most comfortable when at a public gathering (e.g., exhibitions, concerts, movies, etc.)?
15. How would the following factors affect your comfort at being photographed by a professional photographer?
16. How would the following factors affect your comfort at being photographed if the photograph is limited to personal use by the photographer?
17. How would the following factors affect your comfort at being photographed if there are minor children in your vicinity who might also be photographed?
18. How would the following factors affect your comfort at being photographed if the photograph may be published online and you are notified afterwards (e.g. social networks)?
19. How would the following factors affect your comfort at being photographed if the photograph may be posted in a forum with restricted membership (e.g. company/university mailing list)?
20. How would the following factors affect your comfort at being photographed if the photographer is an acquaintance?
21. How would the following factors affect your comfort at being photographed if the photographer is a stranger?
22. How would the following factors affect your comfort at being photographed if you are photographed with acquaintances?
23. How would the following factors affect your comfort at being photographed if photograph may be published online without my knowledge (e.g. social networks)?
24. Are there any other venues or activities, where you have particular privacy desires regarding image capture?
25. As a photographer, would you like to respect the privacy preferences of people around you?
26. Age group
27. Gender
28. Max. Educational level (e.g., high school, some college credits, B.S, MS, Ph.D.)

Figure 9. Bystanders' privacy survey questions.

After the initial survey, participants wore the FacePET wearable and had their photo taken using the rear-facing camera of an iPhone 7 in an indoor setting (i.e., a lab) with the wearable system being active and inactive. The captured photos were then used as input in a Python application that used the OpenCV's face detection Application Programming Interface (API) [26] implementation which provides an open source implementation of the Viola–Jones face detection algorithm [27]. Figure 3 shows screenshots of this application. The results of the face detection were presented to the participants (as Figure 3 shows) before they filled out a second survey (called the "Usability Survey") about the use of the wearable device and their attitudes about it. Figure 10 shows the questions we asked in this second survey. Once this second survey was completed, the participants concluded their participation in the study. A total of $n = 21$ participants took part of this study and we raffled a gift card for USD 25.00 among the participants as an incentive reward for their participation. Table 3 presents the participants' demographics in this study. All participants were at least 18 years old.

Usability Survey

1. On a scale from 1-10, how easy was it to understand and use the wearable device (1=Very easy, 10=Very difficult)?
2. Is the device something you would use daily?
3. If no, would use another version similar to this device?
4. If no, what reasons do you have for not using the device or something similar to the device?
5. What do you think the reactions of the people in your surroundings will be when you are using this device in public?
6. Do you believe that if wearables that conceal users' identities become available, will they
7. allow smart glasses to become more popular (circle one)?
8. Are there any improvements to the device you would recommend?

Figure 10. FacePET's usability/user perceptions survey questions.

Table 3. Participant demographics.

Participants' Characteristics		Number of Participants
Age group	Less than 20 years	1
	20–30 years	17
	30–40 years	3
Gender	Male	14
	Female	7
Educational level	High school	1
	Some college credits	14
	Associate's degree	1
	Bachelor's degree	4
	Master's degree	1

4.2. Study Results

The initial bystanders' privacy survey assessed the participant's knowledge about facial and bystanders' privacy and how it affects them. Participants were first asked questions about how they feel themselves with respect to technology and how often they took pictures and videos. They were also asked how much they knew about the issue of bystanders' privacy and if they found it to be an important issue in today's world. Out of the 21 participants, 19 of them considered themselves to be tech savvy. When asked how often they took pictures/videos, 11 participants *took pictures often* while the rest answered *not so often* (8 participants) or *very little* (2 participants). When asked about bystanders' privacy and how much they knew about bystanders' privacy, surprisingly, most of them *did not know much about the issue* or *not at all* (11 participants adding both choices). In this question, 2 participants stated that they *knew a lot about it* and 7 participants stated that *they knew enough*. After these questions and being introduced to the topic, most of the participants were in agreement *that it is an important issue in today's world* (18 participants), and the rest stating that *it was not* (3 participants).

When asked about the preferred privacy actions in certain contexts such as *being at the gym, in a bar, at the beach*, among others (see Figure 11), the participants were given for each situation five choices *(I agree to be captured in any photograph; I agree to be captured, but please send me a copy of any photograph that includes me; Please obscure my appearance in any photograph that includes me; I can decide my preference only after I see the photograph; I do not wish to be captured in any photograph)*. The most common choice among all contexts was *"I can decide my preference only after I see the photograph"* (32% of all choices). The second most frequent choice was "*I agree to be captured in any photograph*" with 28.07% of all choices). It is worth noting that in general, 15 participants chose a privacy action other than always agreeing to be photographed. This result demonstrates that, among our survey participants, they prefer some type of privacy protection when photographed. In this part of the survey we had a total of 228 answers.

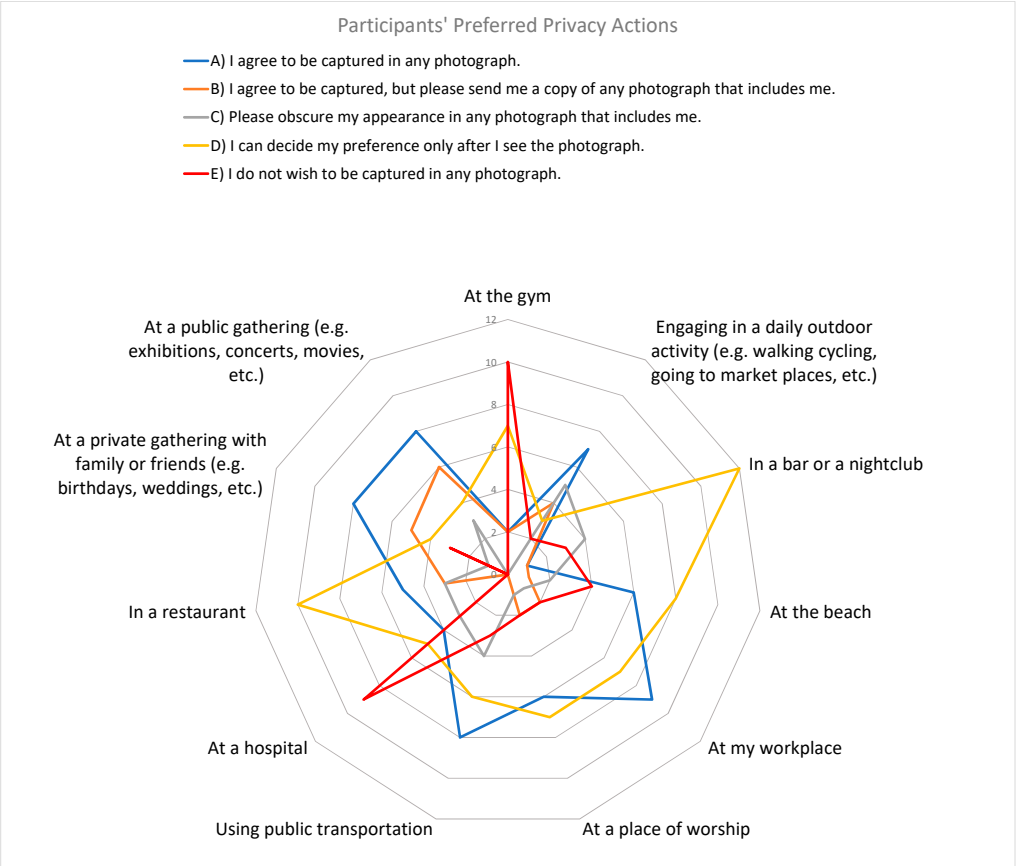


Figure 11. Participants' preferred privacy actions in various contexts. The scale in the radar chart indicate frequency of participants and the lines indicate a context. Vertices indicate a privacy action.

From the results of the survey, we found that the participants of our study prefer to be photographed without restrictions in some communal places and activities such as outdoor activities, workplaces, at private gatherings with known people (i.e., family and friends), while they do not wish to be photograph in places and activities related to health (i.e, at hospitals, at gyms). It worth noting that the most preferred choice for places such as in bars/nightclubs, at the beach, at a place of worship, and in a restaurant was *"I can decide my preference only after I see the photograph"*. These results show that, in health-related activities, and in contexts that involve consumer/lifestyle habits (i.e., bars, beaches, and restaurants) participants of the study want to control their privacy. This conclusion is similar to past works with a focus on bystander's privacy perceptions (as described in Section 2.1).

The last section of the initial bystanders' privacy survey evaluated the participants' comfort levels about who may be a photographer taking photos of them and what the photographer can do with the photos regardless of any specific situation. For each type of photographer/action, the participant could choose five comfort levels (in a Likert scale). Figure 12 shows the results of these questions. In the figure, the Likert scale has been reduced to three categories to simplify the visualization and analysis. In these questions, less comfortable choices (little less and much less) represented 35.24% of all choices, neutral choice ("*I will feel the same*") represented 32.86% of all choices, and more comfortable choices represented 31.9%. In these questions, participants felt more comfortable in situations where there was some type of privacy protection or the photographer was somebody professional or known to the participant. Finally, participants felt less comfortable if the photos were to be published without consent, if the photographer was a stranger, and if there were children in the proximity of the photo. These results demonstrate that participants were concerned about their facial privacy when photos are taken and published without their knowledge. In this part of the survey there were 210 answers.

The results in this part of the study are similar to past works in the area of bystanders' perceptions on photo sharing (see Section 2.1).

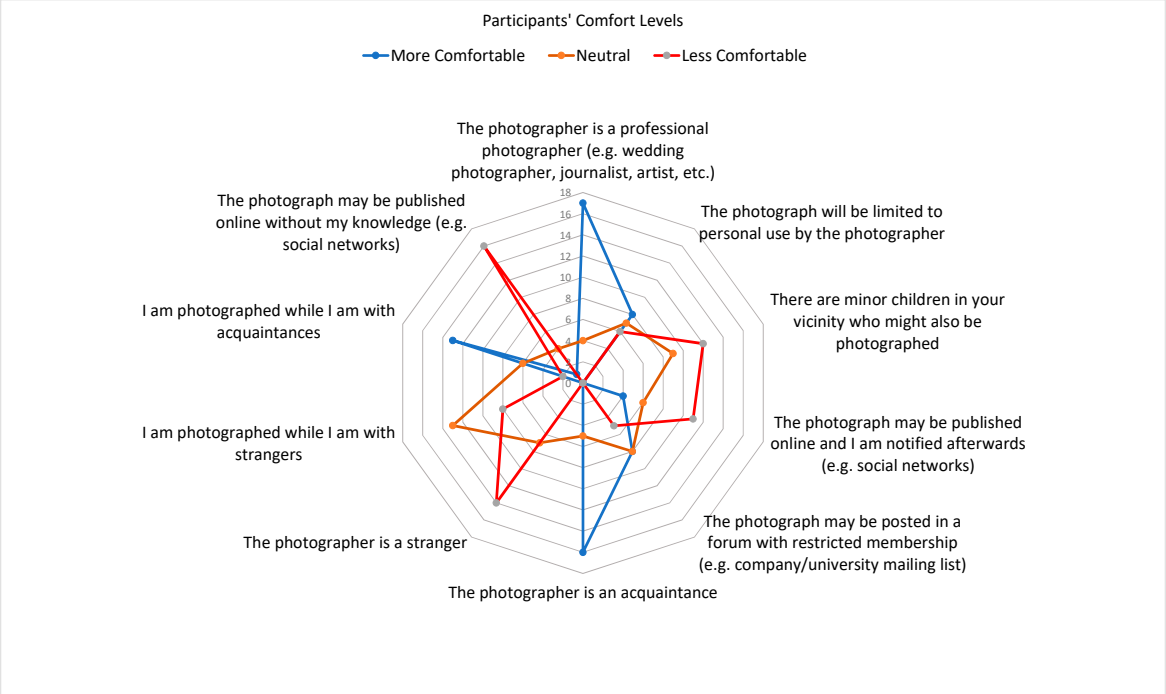


Figure 12. Participants' comfort levels on photographers and actions with photos. The scale in the chart shows the frequency of participants and the lines indicate a comfort level. Vertices indicate a context.

The participants then wore the FacePET system. Each individual was photographed using the rear-facing camera of an Apple iPhone 7 mobile phone with the device enabled (privacy protection) and disabled. These photos were then fed into the OpenCV's face detection script (Figure 3). Out of the 21 participants, six participants' faces were detected, giving the device's a success rate in protecting a user's face around 71%. A handful of the participants also took pictures using their own mobile phones so that comparisons could be made for how effective the device worked regardless of the different cameras. The participants were then shown the results of the application (Figure 3) and then they answered the usability/user perceptions survey shown in Figure 10.

While conducting the experiment on capturing the photos, we noticed that the glasses seemed a little bit big on some of the participants who had thinner or smaller facial structures. This caused OpenCV's face detection script to detect their faces as the FacePET device failed to thwart the facial features. We also observed that the illumination in the room where the experiment was conducted diminished the effectiveness of the device. We plan to address these aspects in the future.

After using the FacePET system and answering the usability survey, 17 participants found the system easy to understand and use. When asked if the device was something they would use on a daily basis, nine participants answered affirmatively, while the rest stated that they would not use the device in its current state. Within the group of participants who answered that they would not use the device (12 participants), we asked if they would use a similar version of the device (one that would achieve the same goals for privacy protection). In this question, 7 out of 12 participants answered affirmatively.

Even though the original FacePET system is not a wearable that most of the participants would use, when adding those participants who initially answered *yes* (9 participants) to use FacePET and those who would use a similar version (7 participants), the majority of the participants (16 participants out of 21) would use FacePET or similar devices (i.e., other bystander-based devices) to protect their facial privacy. Most of the concerns or reasons surrounding participants not wanting to use the device

seemed to be because of the device's form factor. Some of these reasons indicated by the participants included:

- The current model is too big and draws attention.
- The model is not stylish and can obstruct vision.
- Select participants do not really take pictures or engage in the media market in such a manner.

When the participants were asked about how people would react when seeing them wearing the device, a variety of responses given were:

- Person laughs and says, "Stupid glasses".
- People would stare a lot.
- People would be confused at first or creeped out.
- People would ask why the user was wearing such a device.
- The device would only invite more people to take pictures of it.

From these answers, it seems there would be plenty of confusion on others around the user about the purpose of the device and why someone would wear it in its current form factor. Despite the fact that some of the feedback obtained relates specifically on our FacePET prototype, it is worth pointing out that the majority of the participants did agree that if smart glasses had features to conceal users' identities, it would allow such smart glasses to become more popular with 17 participants stating *yes*, 3 participants *feeling indifferent*, and 1 participant stating *no*. Finally, we gathered some suggestions on how to improve our FacePET prototype. Some of the improvements that were repeated among the responses include a more fashionable design, a better size (smaller) for the goggles, and fixing the long wires that connect the power supply with the goggles and the microcontroller in the current prototype.

4.3. Study Limitations

Due to the sample size (n = 21) of our study and because all participants recruited in our study were from Columbus State University, the findings of this study cannot be generalized to a broader population. Thus, if we conduct our study with a broader and more diverse population, we may obtain different results to the ones currently presented in this work. As such, our conclusions are written in terms that relate to our participants rather than a broader population. While our sample size and its characteristics are similar to previous works that also used interviews, testing of devices and the study of users in the wild [8,31,32,34,35,40], we acknowledge that to achieve external validity we will need to scale our experiment to reach a broader population to increase both the sample size and its diversity. To achieve this, we propose as future work the development of an experiment wherein participants do not rely on the FacePET device for the study, but by using current advances in AI in face and eye detection, we could simulate how a participant would look with a bystander-based privacy protection device similar to FacePET, followed by participants interacting with an interface that simulates the device, and finally have participants answer an online survey or record them answering open questions about the simulated device. We plan to conduct this study in our future research works.

5. Conclusions

In this work we conducted a user study to assess user perceptions about the FacePET system or similar bystander-centric devices for facial privacy protection. We conducted our study with 21 participants who took a survey to gather information about facial and bystanders' privacy, privacy choices with cameras, and preferences about sharing photos. Participants then used the FacePET wearable and answered a second survey about the usability and perceptions of the system and/or similar devices. We found evidence that participants want some type of privacy protection when photographed, especially in contexts that involve consumer/lifestyle habits, and they do not wish to be photographed in contexts that involve health-related activities or locations. Participants also showed concerns about their facial privacy when photos are taken and published without their knowledge.

When the participants used the FacePET system, we found that even though they would not use the current prototype on a daily basis because of its bulkiness and unfashionable design, most of the participants agreed that they would use a device similar to FacePET to protect their facial privacy. Participants finally agreed that if smart glasses had features that would allow users to protect their facial privacy, this feature would make smart glasses more popular with the general public.

For future work, we will develop a research study to recruit more participants and address the external validity of the conclusions of our small study. To achieve this, we plan to create a research protocol that does not require the utilization of a physical wearable (e.g., access to a FacePET prototype) to scale the data collection. In addition, based on the results of the FacePET evaluation, we plan to improve the appearance of the FacePET design. Finally, we plan also to improve the facial privacy protection aspects of the device to protect against newer face detection and recognition systems based on deep learning and Convolutional Neural Networks (CNNs).

Author Contributions: Conceptualization, A.J.P. and S.Z.; Funding acquisition, A.J.P.; Investigation, S.G., L.Y.M.G., J.A.M.; Software, L.Y.M.G. and J.A.M.; Supervision, A.J.P.; Writing—original draft, A.J.P. and S.G.; Writing—review and editing, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the U.S Department of Defense and the U.S. National Science Foundation under grant award # 1560214, and by the U.S. National Science Foundation under grant award # 1950416.

Acknowledgments: We thank the anonymous reviewers for their valuable comments, which helped improve the paper's content, quality, and organization.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Perez, A.J.; Zeadally, S.; Griffith, S. Bystanders' privacy. *IT Prof.* **2017**, *19*, 61–65. [CrossRef]
2. Perez, A.J.; Zeadally, S. Privacy issues and solutions for consumer wearables. *IT Prof.* **2018**, *20*, 46–56. [CrossRef]
3. Truong, K.N.; Patel, S.N.; Summet, J.W.; Abowd, G.D. Preventing camera recording by designing a capture-resistant environment. In Proceedings of the International Conference on Ubiquitous Computing, Tokyo, Japan, 11–14 September 2005; pp. 73–86.
4. Tiscareno, V.; Johnson, K.; Lawrence, C. Systems and Methods for Receiving Infrared Data with a Camera Designed to Detect Images Based on Visible Light. U.S. Patent 8848059, 30 September 2014.
5. Wagstaff, J. Using Bluetooth to Disable Camera Phones. Available online: http://www.loosewireblog.com/2004/09/using_bluetooth.html (accessed on 21 September 2018).
6. Kapadia, A.; Henderson, T.; Fielding, J.J.; Kotz, D. Virtual walls: Protecting digital privacy in pervasive environments. In Proceedings of the International Conference Pervasive Computing, LNCS 4480, Toronto, ON, Canada, 13–16 May 2007; pp. 162–179.
7. Blank, P.; Kirrane, S.; Spiekermann, S. Privacy-aware restricted areas for unmanned aerial systems. *IEEE Secur. Priv.* **2018**, *16*, 70–79. [CrossRef]
8. Steil, J.; Koelle, M.; Heuten, W.; Boll, S.; Bulling, A. Privaceye: Privacy-preserving head-mounted eye tracking using egocentric scene image and eye movement features. In Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications, 25–28 June 2019; pp. 1–10.
9. Pidcock, S.; Smits, R.; Hengartner, U.; Goldberg, I. Notisense: An urban sensing notification system to improve bystander privacy. In Proceedings of the 2nd International Workshop on Sensing Applications on Mobile Phones (PhoneSense), Seattle, WA, USA, 12–15 June 2011; pp. 1–5.
10. Yamada, T.; Gohshi, S.; Echizen, I. Use of invisible noise signals to prevent privacy invasion through face recognition from camera images. In Proceedings of the ACM Multimedia 2012 (ACM MM 2012), Nara, Japan, 29 October 2012; pp. 1315–1316.
11. Yamada, T.; Gohshi, S.; Echizen, I. Privacy visor: Method based on light absorbing and reflecting properties for preventing face image detection. In Proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Manchester, UK, 13–16 October 2013; pp. 1572–1577.

12. Sharif, M.; Bhagavatula, S.; Bauer, L.; Reiter, M.K. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In Proceedings of the 2016 ACM SIGSAC Conference Computer and Communications Security (CCS 2016), Vienna, Austria, 24–28 October 2016; pp. 1528–1540.
13. ObscuraCam: Secure Smart Camera. Available online: https://guardianproject.info/apps/obscuracam/ (accessed on 30 September 2018).
14. Aditya, P.; Sen, R.; Druschel, P.; Joon Oh, S.; Benenson, R.; Fritz, M.; Schiele, B.; Bhattacharjee, B.; Wu, T.T. I-pic: A platform for privacy-compliant image capture. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys), Singapore, 25–30 June 2016; pp. 249–261.
15. Roesner, F.; Molnar, D.; Moshchuk, A.; Kohno, T.; Wang, H.J. World-driven access control for continuous sensing. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS 2014), Scottsdale, AZ, USA, 3–7 November 2014; pp. 1169–1181.
16. Maganis, G.; Jung, J.; Kohno, T.; Sheth, A.; Wetherall, D. Sensor Tricorder: What does that sensor know about me? In Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile '11), Phoenix, AZ, USA, 1–3 March 2011; pp. 98–103.
17. Templeman, R.; Korayem, M.; Crandall, D.J.; Kapadia, A. PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces. In Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium, San Diego, CA, USA, 23–26 February 2014; pp. 23–26.
18. AVG Reveals Invisibility Glasses at Pepcom Barcelona. Available online: http://now.avg.com/avg-reveals-invisibility-glasses-at-pepcom-barcelona (accessed on 7 July 2020).
19. Frome, A.; Cheung, G.; Abdulkader, A.; Zennaro, M.; Wu, B.; Bissacco, A.; Adam, H.; Neven, H.; Vincent, L. Large-scale privacy protection in Google Street View. In Proceedings of the 12th International Conference on Computer Vision, Kyoto, Japan, 29 September–2 October 2009; pp. 2373–2380.
20. Li, A.; Li, Q.; Gao, W. Privacycamera: Cooperative privacy-aware photographing with mobile phones. In Proceedings of the 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 27–30 June 2016; pp. 1–9.
21. Schiff, J.; Meingast, M.; Mulligan, D.K.; Sastry, S.; Goldberg, K. Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, San Diego, CA, USA, 29 October–2 November 2007; pp. 65–89.
22. Ra, M.R.; Lee, S.; Miluzzo, E.; Zavesky, E. Do not capture: Automated obscurity for pervasive imaging. *IEEE Internet Comput.* **2017**, *21*, 82–87. [CrossRef]
23. Ashok, A.; Nguyen, V.; Gruteser, M.; Mandayam, N.; Yuan, W.; Dana, K. Do not share! Invisible light beacons for signaling preferences to privacy-respecting cameras. In Proceedings of the 1st ACM MobiCom Workshop on Visible Light Communication Systems, Maui, HI, USA, 7–11 September 2014; pp. 39–44.
24. Ye, T.; Moynagh, B.; Albatal, R.; Gurrin, C. Negative face blurring: A privacy-by-design approach to visual lifelogging with google glass. In Proceedings of the 23rd ACM International Conference on Information and Knowledge Management, Shanghai, China, 3–7 November 2014; pp. 2036–2038.
25. Perez, A.J.; Zeadally, S.; Matos Garcia, L.Y.; Mouloud, J.A.; Griffith, S. FacePET: Enhancing bystanders' facial privacy with smart wearables/internet of things. *Electronics* **2018**, *7*, 379. [CrossRef]
26. Face Detection Using Haar Cascades. Available online: https://docs.opencv.org/3.4.2/d7/d8b/tutorial_py_face_detection.html (accessed on 7 July 2020).
27. Viola, P.; Jones, M. Robust real-time face detection. *Int. J. Comput. Vis.* **2004**, *57*, 137–154. [CrossRef]
28. Office of the Privacy Commissioner of Canada. Consent and Privacy a Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic Documents Act. Available online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605 (accessed on 9 September 2020).
29. United States the White House Office. National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy. Available online: https://www.hsdl.org/?collection&id=4 (accessed on 9 September 2020).
30. Horizon 2020 Horizon Programme of the European Union. Complete Guide to GDPR Compliance. Available online: https://gdpr.eu/ (accessed on 9 September 2020).

31. Palen, L.; Salzman, M.; Youngs, E. Going wireless: Behavior & practice of new mobile phone users. In Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work (CSCW'00), Philadelphia, PA, USA, 2–6 December 2000; pp. 201–210.
32. Denning, T.; Dehlawi, Z.; Kohno, T. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing System, Toronto, ON, Canada, 26 April 26–1 May 2014; pp. 2377–2386.
33. Motti, V.G.; Caine, K. Users' privacy concerns about wearables. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 30 January 2015; pp. 231–244.
34. Hoyle, R.; Templeman, R.; Armes, S.; Anthony, D.; Crandall, D.; Kapadia, A. Privacy behaviors of lifeloggers using wearable cameras. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, WA, USA, 13–17 September 2014; pp. 571–582.
35. Hoyle, R.; Stark, L.; Ismail, Q.; Crandall, D.; Kapadia, A.; Anthony, D. Privacy norms and preferences for photos Posted Online. *ACM Trans. Comput. Hum. Interact. (TOCHI)* **2020**, *27*, 1–27. [CrossRef]
36. Zhang, S.A.; Feng, Y.; Das, A.; Bauer, L.; Cranor, L.; Sadeh, N. Understanding people's privacy attitudes towards video analytics technologies. In Proceedings of the FTC PrivacyCon 2020, Washington, DC, USA, 21 July 2020; pp. 1–18.
37. Hatuka, T.; Toch, E. Being visible in public space: The normalisation of asymmetrical visibility. *Urban Stud.* **2017**, *54*, 984–998. [CrossRef]
38. Wang, Y.; Xia, H.; Yao, Y.; Huang, Y. Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the US. In Proceedings of the on Privacy Enhancing Technologies, Darmstadt, Germany, 16–22 July 2016; pp. 172–190.
39. Chang, V.; Chundury, P.; Chetty, M. Spiders in the sky: User perceptions of drones, privacy, and security. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 6–11 May 2017; pp. 6765–6776.
40. Ahmad, I.; Farzan, R.; Kapadia, A.; Lee, A.J. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proc. ACM Hum. Comput. Interact.* **2020**, *4*, 116. [CrossRef]
41. Nielsen, J. *Usability Engineering*, 1st ed.; Academic Press: Cambridge, MA, USA, 1993; ISBN 978-0125184052.
42. Zeadally, S.; Khan, S.; Chilamkurti, N. Energy-efficient networking: Past, present, and future. *J. Supercomput.* **2012**, *62*, 1093–1118. [CrossRef]
43. Jamil, F.; Kim, D.H. Improving accuracy of the alpha–beta filter algorithm using an ANN-based learning mechanism in indoor navigation system. *Sensors* **2019**, *19*, 3946. [CrossRef] [PubMed]
44. Ahmad, S.; Kim, D.-H. Toward accurate position estimation using learning to prediction algorithm in indoor navigation. *Sensors* **2020**, *20*, 4410.
45. Jarvis, J. *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live*, 1st ed.; Simon & Schuster: New York, NY, USA, 2011; pp. 1–272. ISBN 978-1451636000.
46. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.H. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef] [PubMed]
47. Iqbal, M.A.; Amin, R.; Kim, D. Adaptive thermal-aware routing protocol for wireless body area network. *Electronics* **2019**, *8*, 47.
48. Dalvi, N.; Domingos, P.; Sanghai, S.; Verma, D. Adversarial classification. In Proceedings of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Seattle, WA, USA, 22–25 August 2004; pp. 99–108.
49. Biggio, B.; Roli, F. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognit.* **2018**, *84*, 317–331. [CrossRef]
50. Li, H.; Lin, Z.; Shen, X.; Brandt, J.; Hua, G. A convolutional neural network cascade for face detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Boston, MA, USA, 7–22 June 2015; pp. 5325–5334.
51. Bose, A.J.; Aarabi, P. Adversarial attacks on face detectors using neural net based constrained optimization. In Proceedings of the IEEE 20th International Workshop on Multimedia Signal Processing (MMSP), Vancouver, BC, Canada, 29–31 August 2018; pp. 1–6.

52. Goswami, G.; Ratha, N.; Agarwal, A.; Singh, R.; Vatsa, M. Unravelling robustness of deep learning based face recognition against adversarial attacks. In Proceedings of the 32nd AAAI Conference on Artificial Intelligence (AAAI-18), New Orleans, LA, USA, 2–7 February 2018; p. 6829.
53. Zeadally, S.; Siddiqui, F.; Baig, Z. 25 years of bluetooth technology. *Future Internet* **2019**, *11*, 194. [CrossRef]