



University of Kentucky
UKnowledge

Information Science Faculty Publications

Information Science

12-3-2018

FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things

Alfredo J. Perez
Columbus State University

Sherali Zeadally
University of Kentucky, szeadally@uky.edu

Luis Y. Matos Garcia
Universidad del Turabo, Puerto Rico

Jaouad A. Mouloud
Bergen Community College

Scott Griffith
Columbus State University

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Follow this and additional works at: https://uknowledge.uky.edu/slis_facpub

 Part of the [Digital Communications and Networking Commons](#), [Electrical and Computer Engineering Commons](#), and the [Information Security Commons](#)

Repository Citation

Perez, Alfredo J.; Zeadally, Sherali; Garcia, Luis Y. Matos; Mouloud, Jaouad A.; and Griffith, Scott, "FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things" (2018). *Information Science Faculty Publications*. 51.
https://uknowledge.uky.edu/slis_facpub/51

This Article is brought to you for free and open access by the Information Science at UKnowledge. It has been accepted for inclusion in Information Science Faculty Publications by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things

Notes/Citation Information

Published in *Electronics*, v. 7, issue 12, 379, p. 1-19.

© 2018 by the authors. Licensee MDPI, Basel, Switzerland.


This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Digital Object Identifier (DOI)

<https://doi.org/10.3390/electronics7120379>

Article

FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things

Alfredo J. Perez ^{1,*}, Sherali Zeadally ², Luis Y. Matos Garcia ³, Jaouad A. Mouloud ⁴ and Scott Griffith ⁵

¹ TSYS School of Computer Science, Columbus State University, Columbus, GA 31907, USA

² College of Communication and Information, University of Kentucky, Lexington, KY 40506, USA; szeadally@uky.edu

³ Department of Electrical and Computer Engineering, Universidad del Turabo, Gurabo, PR 00777, USA; lmatosgarcia2@gmail.com

⁴ Department of Information Technology, Bergen Community College, Paramus, NJ 07652, USA; ahm.jaouad@gmail.com

⁵ TSYS School of Computer Science, Columbus State University, Columbus, GA 31907, USA; griffith_scott@columbusstate.edu

* Correspondence: perez_alfredo@columbusstate.edu; Tel.: +1-706-334-8194

Received: 28 October 2018; Accepted: 29 November 2018; Published: 3 December 2018



Abstract: Given the availability of cameras in mobile phones, drones and Internet-connected devices, facial privacy has become an area of major interest in the last few years, especially when photos are captured and can be used to identify bystanders' faces who may have not given consent for these photos to be taken and be identified. Some solutions to protect facial privacy in photos currently exist. However, many of these solutions do not give a choice to bystanders because they rely on algorithms that de-identify photos or protocols to deactivate devices and systems not controlled by bystanders, thereby being dependent on the bystanders' trust in these systems to protect his/her facial privacy. To address these limitations, we propose FacePET (Facial Privacy Enhancing Technology), a wearable system worn by bystanders and designed to enhance facial privacy. We present the design, implementation, and evaluation of the FacePET and discuss some open research issues.

Keywords: face detection; face recognition; internet of things; bystanders' privacy; privacy enhancing technology; smart glasses; wearables

1. Introduction

According to Ericsson's Mobility Report [1], there are more than four billion smartphones subscriptions in the world. The availability of these devices with high-resolution cameras, mobile Internet connectivity, and the development of artificial intelligence techniques such as deep learning can expose individuals to privacy issues. Among these issues is bystanders' privacy [2,3] which is the issue that arises when a device collects sensor data (such as photos, sound or video) that can be used to identify bystanders who may have not given consent for them to be identified.

The origins of the problem of bystanders' privacy can be traced back to the development of cameras that took photos in the late 19th century. However, in recent years, taking photographs in public that may include bystanders has once again been receiving attention, especially when it comes to privacy concerns of the bystanders. This problem has become important because of the ubiquity of camera-enabled mobile and wearable devices, and the proliferation of social networks that allow photos to be instantly shared with the world instead of being kept private in a physical album (as was the case only a few decades ago) [2]. An example where bystanders were identified by using photos

of their faces without consent was the incident that occurred in 2016 when a Russian photographer took photos of bystanders at a subway station and was able to identify them using free software available on the Internet [4]. The bystanders later knew about their identification through news reports. This example underscores the risks that people are exposed to with respect to their facial privacy as mobile devices become even more affordable, powerful, and ubiquitous. It is worth noting that this issue arises with any camera-enabled Internet of Things (IoT) device such as web/security cameras and drones.

Privacy in mobile, wearable and IoT devices usually focus on attacks and solutions to protect a user's private space from unauthorized parties' access, and the protection of private data in social networking sites and other Internet services. For the facial privacy of bystanders, however, there is a social aspect that extends the user's private space: when photos, videos, and sound are collected in shared spaces (especially in public spaces such as parks or restaurants), a conflict of ownership of spaces arises between the user and the bystanders. Using devices that can collect identifiable data creates the perception of ownership of the space surrounding the device (by the user of the device), which can include the space surrounding bystanders [5–8].

In the early 2000s, research on human-computer interaction found that the use of cellphones in public spaces was offensive to some people [9], because these devices presented a conflict of social spaces where a user is simultaneously in the physical space that he or she occupies, and the virtual space of the conversation over the cellphone. Today, many wearable devices such as smart glasses also include cameras and microphones that create strong privacy concerns [10] when collecting and sharing data over the Internet without permission, thereby directly threatening bystanders' space and autonomy. Table 1 outlines and explains bystanders' fears and concerns in greater detail.

Table 1. Bystanders' privacy concerns adapted from Motti et al. [10].

Privacy Concern	Description
Facial recognition	Association and recognition of a bystander to a place or a situation where the bystander would not wish to be recognized by others
Social implications	Unawareness by a network of friends regarding data being collected about them
Social media sync	Immediate publishing or sharing without the bystander's knowledge
User's fears: surveillance and Sousveillance	Continuous tracking of activities that might make a user/bystander feel that no matter what he or she does, everything is recorded
Speech disclosure	Capturing speech that a user or bystanders would not want to record or share
Surreptitious A/V recording	Recording audio or video without permission that might affect bystanders
Location disclosure	Fear of inadvertently sharing a location to third parties that should not have access to the location information

Given the importance of bystanders' facial privacy nowadays, this work describes the Facial Privacy Enhancing Technology (FacePET) system, a wearable system worn by bystanders and designed to enhance facial privacy. The main research domain of this work is privacy, with reference disciplines being computer networks and communications (Internet of things and wearables), computer vision (methods to thwart face detection, adversarial machine learning), security (privacy and access control), and human-computer interaction (Internet-connected cameras and wearables in shared spaces).

Our Research Contributions

We summarize the main contributions of this paper as follows:

- We present a taxonomy of recently proposed techniques aimed at enhancing the facial privacy of bystanders.
- We describe and evaluate the design of a wearable device called Facial Privacy Enhancing Technology (FacePET) that enhances the facial privacy of its wearer. To the best of our knowledge, this is the first work that describes an IoT device to enhance the privacy of its wearer.
- We describe a protocol over Bluetooth that provides FacePET's users a way to provide consent to third parties who may want to take photos of them.

The rest of the paper is organized as follows. Section 2 presents a taxonomy of methods that have been proposed to protect the facial privacy of bystanders. In Section 3 we describe FacePET. Section 4 presents an evaluation FacePET. In Section 5 we describe some of the limitations of FacePET and future work. Finally, in Section 6 we present some concluding remarks.

2. Related Work

Methods currently available to handle bystanders' facial privacy can be classified into two broad categories: *location-dependent methods*, which deny third party devices the opportunity to collect data and *obfuscation-dependent methods*, which prevent bystanders' facial detection and identification. Figure 1 shows the taxonomy we used in this paper to classify the methods to protect bystanders' facial privacy. At the end of this section we evaluate the methods for each major category of the taxonomy.

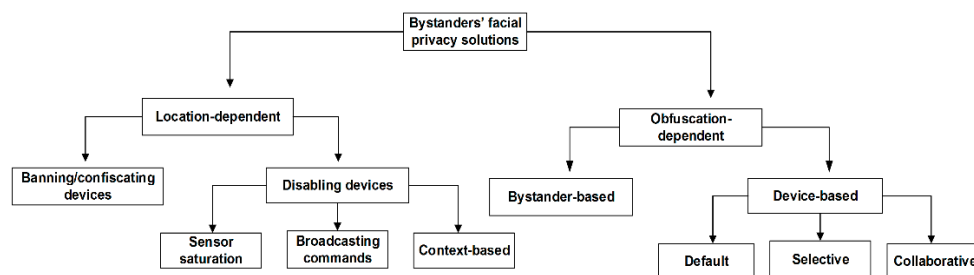


Figure 1. Taxonomy of methods for bystanders' privacy protection [2].

2.1. Location Dependent Methods

Location-dependent methods deny the collection of data at particular shared spaces (such as restaurants, casinos, or cafes). Implementation of this method entails restricting and banning devices' use through warning signs, confiscating devices before entering a shared space, or temporarily disabling user devices in a shared space. According to the taxonomy presented in Figure 1, these methods can be further classified into two categories, namely, (1) banning/confiscating devices and (2) disabling devices.

In the banning/confiscating devices category, third-party devices are confiscated or banned for usage at a shared space. This method has been in use since the end of the 19th century when the use of cameras was forbidden at private beaches and, for some time, at public spaces in the U.S. [11]. When devices cannot be used at the shared space, the bystanders' facial privacy is protected.

In the disabling devices category, bystanders' facial privacy is protected because third-party devices cannot collect data about the bystanders. Devices can be disabled in shared spaces by using three approaches: sensor saturation, broadcasting commands, and context-based approaches. In the first approach (sensor saturation), the goal is to make the sensors of a third-party devices detect an input signal that is greater than the maximum possible measurable input supported by third-party devices' sensors (thereby making the sensors unusable by saturation). An example in this category is

the use of near-infrared pulsating lights from fixed devices at shared spaces directed at the device's camera lens [12] in order to saturate the Charge-Coupled Device (CCD) sensor. Facial privacy is preserved because data cannot be collected when the device's sensor saturates. In the second approach (broadcasting commands) in the disabling devices category, the third-party devices receive some type of command broadcast by a fixed device in the shared space to temporarily disable the capture of facial data. An example in this category is the use of Bluetooth and infrared protocols to send disabling commands [13,14]. In the last category (context-based approaches) of location-dependent methods, third-party devices perform some type of context recognition to trigger software actions that deny the explicit collection of data by disabling user devices' sensors at shared spaces. An example in this category includes the virtual walls approach [15] wherein the device uses contextual information (such as Global Positioning System (GPS) location data) to trigger software actions that can temporarily disable its sensors based on pre-programmed contextual rules. A second example in this group is the system developed by Blank et al. [16] in which camera-enabled drones are restricted from flying over certain areas through rules established in a website and broadcast to the drones. In this case, bystanders' facial privacy is preserved because data cannot be collected by third-party devices when the contexts are recognized and the device's sensors are disabled.

2.2. Obfuscation Dependent Methods

Obfuscation methods attempt to hide the identity of bystanders to avoid their identification. These methods can be classified into two groups: (1) bystander-based obfuscation; and (2) device-based obfuscation.

In bystander-based obfuscation, the bystanders take actions to avoid their facial identification. This might be accomplished by wearing some type of hardware (or clothing) that hides or perturbs the bystanders' identifiable features needed to perform identification, or by having bystanders perform some type of physical action (for example, leaving the shared space, or asking a user to stop using a device) to protect their privacy when bystanders become aware of a device's use in their surroundings that might infringe upon their privacy [17]. Examples in this category include the PrivacyVisor glasses [18,19] that hide facial features using near-infrared light or reflective materials, and the utilization of wearables to impersonate or to hide facial features to deceive facial detection and recognition algorithms [20]. Notification methods that alert bystanders to protect their privacy include the use of Light Emitting Diodes (LEDs) on wearables (such as Snap spectacles) to notify bystanders of video or audio being recorded in their surroundings, and the use of short-range radio broadcasts and WiFi-based communication protocols to notify bystanders about sensing activity being performed in their proximity (e.g., NotiSense [17]).

In the last group (device-based obfuscation), the software at third-party devices adds noise (such as blurring) on collected data to hide bystanders' facial identifiable features. The software at users' devices might perform obfuscation by default (for example, performing blurring all faces detected in a photo or a video), it might let users add noise to obfuscate bystanders selectively (selective obfuscation) [21], or the software on the users and bystanders' devices might access protocols over wireless networks to communicate privacy settings such that the software on the user device could automatically hide bystanders' identifiable features based on these privacy settings (collaborative obfuscation) [22]. The drawback of device-based obfuscation is that bystanders might have no control over the protection of their privacy because device-based obfuscation methods rely on third-party devices.

2.3. Evaluation of Methods for Facial Privacy Protection

Although several solutions to address the issue of bystanders' facial privacy have been proposed in the past (as described in the previous sections), these solutions vary in their efficacy because of the following factors:

- Usability: In human-computer interaction, usability is described as how easily a system can be used by a typical consumer/user to fulfill its objectives [23]. In systems that enhance bystanders' facial privacy, minimal user intervention should be required by the bystander.
- Power consumption: In any type of battery-powered system, power consumption plays a substantial role because devices that deplete their battery in a fast manner need to be recharged often. Since many solutions for bystanders' facial privacy protection involve the utilization of algorithms in mobile devices, power consumption is a design issue for such systems [24].
- Effectiveness: Solutions to protect bystanders' facial privacy involve components and algorithms to identify contexts/faces (to blur or obfuscate them), while others involve extra devices or mechanisms combined with intelligent algorithms. Since these systems make use of artificial intelligence algorithms (i.e., classification algorithms) to detect these contexts and/or faces, the solutions may include false detections or misclassifications which affect the effectiveness and accuracy of the system.

Based on these issues, we evaluate below recent systems and techniques that have been proposed for protecting bystanders' facial privacy by using the ratings shown in Table 2. Table 3 summarizes the evaluated methods/systems along with their corresponding ratings.

Table 2. Design issues for bystanders' facial privacy solutions.

Design Issue	Description	Rating
Usability	Is the method easy to use?	Low, Medium, High
Power consumption	Does the method require high power consumption?	Low, Medium, High
Effectiveness	Is the method effective to protect bystanders?	Low, Medium, High

3. FacePET: Enhancing Facial Privacy with Smart Wearables

3.1. Face Detection and Recognition

Face detection and recognition dates back from the 1970's [25,26], but the advent of imaging sensors embedded in smartphones and digital cameras in conjunction with social networks have paved the way for more research on these algorithms the last decade. Private companies (e.g., Facebook [27]) in addition to law enforcement agencies [28,29] are using algorithms to detect faces for business and law enforcement purposes. In computer vision and image processing, face detection involves detecting if a face is present in a photo/video, whereas face recognition associates a face in a photo/video with an identity.

Figure 2 illustrates the basic steps involved in the detection and recognition of faces in photos and/or video recordings. Initially a photo or video is captured using some type of digital camera embedded in an Internet of Things (IoT) device such as a mobile phone, a drone, or Internet-connected camera (image capture phase). Then, this digital photo/video is passed through some software that checks if there is a face present in the photo/video (face detection phase). Finally, if the face is detected, then the face recognition phase is performed whose output yields the identity of the detected face.

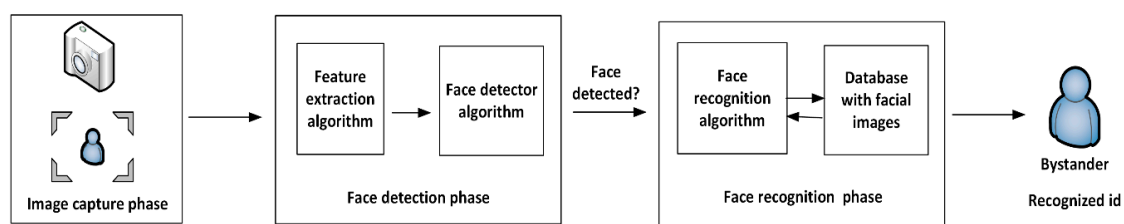


Figure 2. Processes for face detection and recognition.

Table 3. Methods for bystanders' facial privacy protection.

Method	Category	Usability	Power	Effectiveness	Limitations
BlindSpotCapture-resistant environment [12]	Location (disabling, sensor saturation)	High	Low	Low	Utilization of InfraRed (IR) light to disable CCD sensors may not be useful with IR filters on modern cameras.
Disabling devices via infrared [13]	Location (disabling, broadcasting of commands)	High	Low	Medium	Method requires third-party devices to receive IR commands and software to disable sensors which not all third-party devices may have the capability.
Disabling devices via Bluetooth [14]	Location (disabling, broadcasting of commands)	High	Medium	Medium	Method requires third-party devices to receive Bluetooth commands and software to disable sensors which not all third-party devices may have the capability.
Virtual Walls [15]	Location (disabling, context-based)	Medium	High	Medium	Method requires bystanders to set up privacy rules that are accessed in third-party devices. Use of sensors in the mobile device to determine contexts may consume large amounts of power.
Privacy-restricted areas [16]	Location (disabling, context-based)	Medium	Medium	Medium	Method requires bystanders to set up privacy rules that are accessed in third-party devices. Proposed for unmanned aerial vehicles.
World-driven access control [30]	Location (disabling, context-based)	High	High	Medium	Method does not require bystanders' intervention but device may not detect contexts correctly.
Sensor Tricorder [31]	Location (disabling, context-based)	High	High	Medium	Does not require bystanders' intervention but device may not detect contexts correctly. Makes use of Quick Response (QR) codes to encode location privacy rules.
PlaceAvoider [32]	Location (disabling, context-based)	Medium	High	Medium	Requires machine learning algorithms to detect sensitive contexts. May not detect contexts correctly. Devices must have software to detect contexts. Requires third-party user intervention to check if areas are indeed sensitive.
NotiSense [17]	Obfuscation-based (bystander-based)	Medium	Low	Medium	Requires third-party devices to notify bystanders about possible privacy violations and have the bystander to take action to protect his/her facial privacy.
PrivacyVisor [18]	Obfuscation (bystander-based)	High	High	Low	Uses IR in wearables worn by bystanders to obfuscate facial features. IR can be blocked using filters.
PrivacyVisor III [19]	Obfuscation (bystander-based)	High	Low	High	Uses reflective materials in wearables used by bystanders to corrupt photos taken about them.

Table 3. Cont.

Method	Category	Usability	Power	Effectiveness	Limitations
Perturbed eyeglass frames [20]	Obfuscation (bystander-based)	High	High	Medium	Uses patterns in glasses' frames to confuse facial recognition algorithms. May be prone to re-identification.
Invisibility Glasses [33]	Obfuscation (bystander-based)	High	High	Low	Uses IR in wearables worn by bystanders to obfuscate facial features. Needs high power and IR can be blocked using IR filters which are available for mobile phones.
Privacy Protection in Google StreetView [34]	Obfuscation (device-based, default)	High	Low	High	This technology does not depend on the bystander but on the company collecting photos. Company performs obfuscation in the cloud after the photos have been forwarded from the device that captured them.
ObscuraCam [21]	Obfuscation (device-based, selective)	High	High	Medium	This technology blurs faces in photos through a mobile application. Face blurring occurs at the mobile phone and depending of the blurring technique bystanders could be re-identified.
I-pic [22]	Obfuscation (device-based, collaborative)	Medium	High	Medium	Uses protocols between bystander and third-party devices to allow/deny blurring based on privacy rules. Face blurring occurs at the mobile phone and depending on the blurring technique, bystanders could be re-identified.
PrivacyCamera [35]	Obfuscation (device-based, collaborative)	Medium	High	Medium	Uses protocols between the bystander and third-party device to allow/deny blurring based on privacy rules. Face blurring occurs at the mobile phone and depending on the blurring technique bystanders could be re-identified.
Respectful Cameras [36]	Obfuscation (device-based, selective)	High	Low	High	Bystanders use visual colored cues to inform capturing device of privacy rules. Developed for fixed cameras. Face is fully hidden.
Do Not Capture [37]	Obfuscation (device-based, collaborative)	Medium	High	Medium	Uses protocols between the bystander and third-party device to allow/deny blurring based on privacy rules. Face blurring occurs at the mobile phone and depending of the blurring technique the bystanders could be re-identified.
Invisible Light Beacons [38]	Obfuscation (device-based, selective)	High	High	Low	Bystanders use wearable IR beacons to inform capturing devices of privacy rules. Mobile devices with IR filters will ignore the signal sent by the beacons.
Negative face blurring [39]	Obfuscation (device-based selective)	Medium	Low	Medium	Once captured and stored, blurring of bystanders' faces occur when photos are presented through social networks using stored privacy rules.

The development of fast and practical implementations of face detection algorithms in portable devices has been possible through the work of Viola–Jones who developed a face detector that became a standard technique for this task [40]. Viola–Jones’ work is based on three main ideas [41]: (1) the utilization of an image representation (a data structure called “integral image”) that facilitates the extraction of simple features (called “Haar-like features”); (2) the utilization of a simple and efficient classifier based on the AdaBoost machine learning algorithm to select the most promising features to detect faces; and (3) the utilization of a combination of classifiers organized in sequence (called “cascade classifiers”) which allows to quickly discard regions of the image while concentrating on the most promising regions where faces may lie [41]. In the algorithm, a Haar-like feature is calculated as follows [19]:

$$h(r_1, r_2) = s(r_1) - s(r_2) \tag{1}$$

where $s(r_1)$ is the average of the intensities of the pixels in the “white” regions, and $s(r_2)$ is the average of the pixel intensities in the “black” regions as specified by patterns defined by a Haar-like feature. In their paper, Viola–Jones use the basic Haar-like features shown in Figure 3.

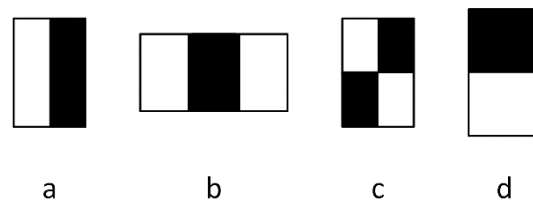


Figure 3. Haar-like features in the Viola and Jones face detection algorithm [41].

The goal in using these features is to guide the face detection algorithm to find better regions of interest in which a face may possibly lie. Before this algorithm was developed, other algorithms already did face detection, but they relied on techniques using pixel positions and relationships between pixels in an image. Such techniques incur a higher computational cost than the Viola–Jones’ approach [40].

The Viola–Jones algorithm calculates the values of these Haar-like features by making use of windows (sub-regions) with different sizes from the original image. Once the features are calculated for all windows, the windows are passed through a classifier that outputs “true” for those windows that may contain a face or “no” otherwise. The goal is to discard windows that may not contain faces. The classifier is built as a sequence (cascade) of (weak) classifiers (Figure 4) in which each consecutive classifier is stronger than the previous one. These weak classifiers have been previously trained before the face detection phase is executed by using the AdaBoost algorithm [41]. Once the windows classified with “yes” have been labeled by the cascade classifier, they may be passed to more complex algorithms.

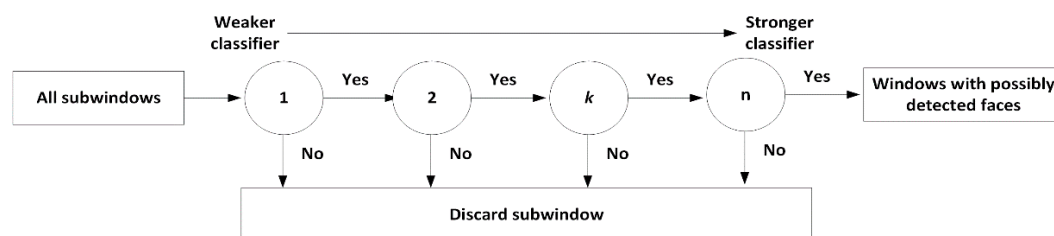


Figure 4. Cascade classifiers in Viola–Jones [40].

3.2. Proposed FacePET System

In this section we describe the proposed Facial Privacy Enhancing Technology (FacePET) system. The FacePET system is based on the idea that bystanders’ facial privacy should be handled by the bystander instead of relying on third-party devices to control bystanders’ facial privacy. To this end,

we have developed a prototype of a smart wearable device that uses visible light to create noise to distort the Haar-like features used by face detection algorithms. Therefore, our wearable device allows bystanders to protect their privacy.

We have incorporated a Bluetooth Low Energy (BLE) microcontroller that controls when the lights are enabled/disabled based on privacy rules established by the bystander. The goal regarding the utilization of the BLE microcontroller is for the bystander to provide consent to third-party devices who may want to take photos of the bystander. Our work is similar to the work of Yamada et al. [18] but with the following differences:

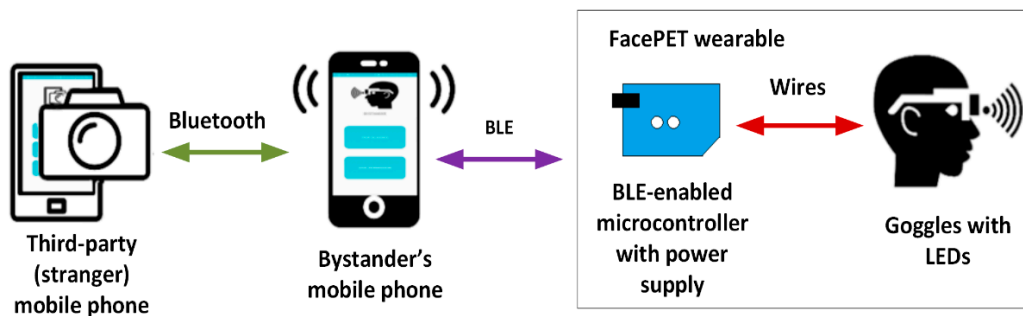
- In Yamada's work [18] the authors proposed the use of near-infrared light to saturate the Charged-Coupled Device (CCD) sensor of digital cameras to distort the Haar-like features. In contrast, our work uses visible light. The reason for using visible light is that newer cameras in smart phones (e.g., Apple's iPhone 4 and newer devices) and other devices may include an IR filter that blocks the intended noise if IR light is used. This makes their device unsuccessful in protecting bystanders' facial privacy.
- Our system includes a BLE microcontroller for the bystander to control an Access Control List (ACL) in which the bystander can set up permissions for third-party devices to take photos without the noise (temporarily disabling the FacePET wearable), hence creating a "smart" wearable.
- We developed a bystander consent protocol over Bluetooth that enables communication between the bystander and third-party devices to provide and exchange privacy consents.

3.2.1. FacePET System's Hardware Architecture

The hardware architecture of the FacePET system (shown in Figure 5) includes the following components:

- *Goggle with LEDs*: The goggles are equipped with LEDs that are turn on/off by the microcontroller. To avoid physical discomfort to the bystander when using the goggles and the LEDs are turned on, the goggles' lenses should have a filter tuned to the wavelength of the LEDs on the goggles. The LEDs on the goggles are connected to the BLE-enabled microcontroller through wires which also provide power to them.
- *BLE-enabled microcontroller*: This component controls the LEDs on the goggle and connects to the bystander's mobile phone via Bluetooth Low Energy (BLE). The microcontroller has its own power supply independent of the one in the bystanders' mobile phone that also provides power to the LEDs. Depending on the privacy protocols implemented, the microcontroller may have the software that implements the Access Control List (ACL) to disable the LEDs, or the ACL may be implemented at the bystanders' mobile phone software. The FacePET wearable device is composed of the BLE microcontroller and the goggles (as shown in Figure 5).
- *Bystanders' mobile phone*: The bystanders' mobile phone executes software that configures the wearable's microcontroller. In addition to configuring the wearable, the bystanders' mobile phone executes software that provides consent to third-parties to turn off the LEDs when an authorized third party wishes to take a photo with the bystander in it. Depending on the privacy protocols implemented, when an authorized third-party wishes to take a photo with the bystander, the ACL may be implemented in the bystander's mobile phone or the third-party may communicate directly with the wearable. The bystanders' mobile phone communicates via BLE with the microcontroller and it communicates with third-party mobile phones via Bluetooth. In future implementations this communication between smartphones may also be Wi-Fi or IP-based.
- *Third-party (stranger) mobile phone*: The third-party (stranger) mobile phone is used by a third-party to request consent for photos to be taken about the bystander. In our current implementation these consents are requested via Bluetooth to the bystanders' mobile phone prior to the third-party can take a photo of the bystander. If consent is given by the bystander, when the third-party mobile

phone is about to take a photo of the bystander, it communicates with the bystander device again to request the LEDs of the goggle to be turned off (if consent has been previously given).



Acronyms

FacePET: Facial Privacy Enhancing Technology

BLE: Bluetooth Low Energy

LED: Light Emitting Diode

Figure 5. FacePET system’s hardware architecture.

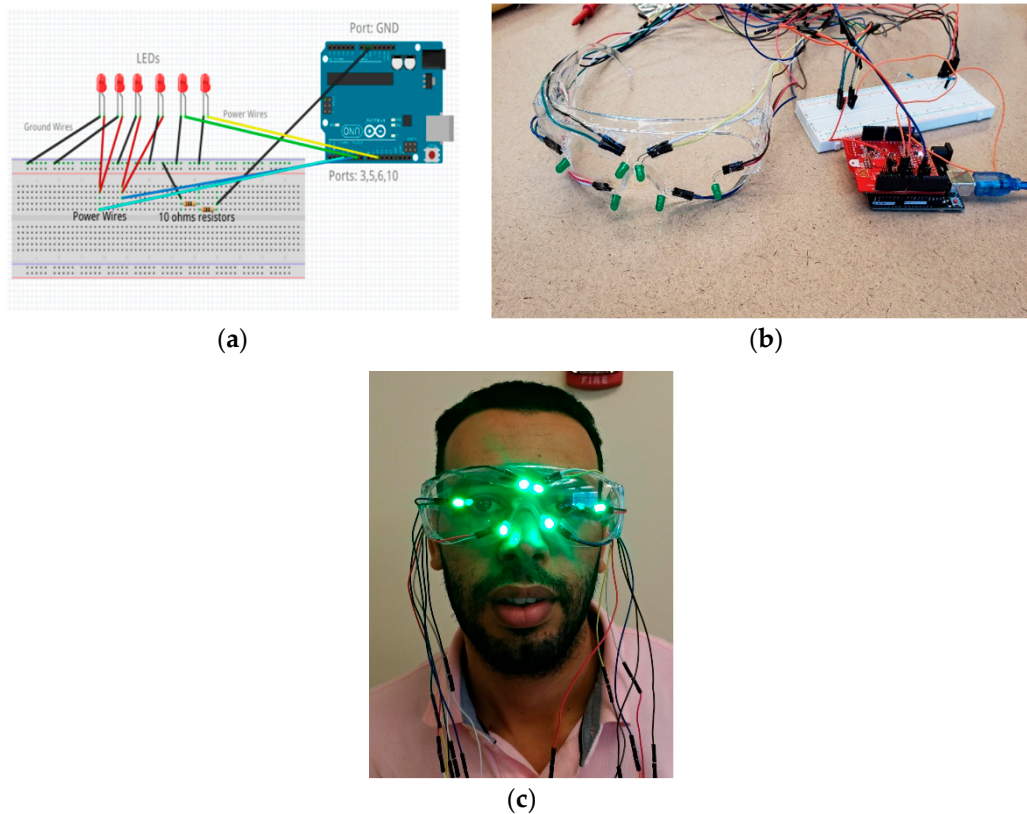


Figure 6. The FacePET wearable device. (a) Wiring sketch diagram for FacePET LEDs; (b) Goggle with LEDs and BLE microcontroller; (c) FacePET wearable prototype worn by a bystander (the person in the photo is one of the authors).

In our current prototype (shown in Figure 6) we used safety goggle bought at a local hardware store. We placed six LEDs on the goggle as shown in Figure 6c. Initially we tried IR LEDs, but they were discarded when we found that the Apple iPhone 4 and newer versions of the iPhone include an IR filter for their rear-facing camera (possibly IR filters will become a standard feature in future mobile phones). Consequently, we tested red, green and blue LEDs for our prototype. Figure 6a shows the wiring sketch diagram for the Arduino board and the LEDs. For the BLE-enabled microcontroller

in the prototype, we used an Arduino Uno [42] with the Seedstudio Bluetooth 4.0 Low Energy-BLE Shield v2.1 [43] (Figure 6b). The Arduino's power supply used was a battery pack connected to the Arduino's USB B port. We used smartphones with the support of BLE running Android 6 (or better). Figure 6c shows a bystander using the FacePET wearable device.

3.2.2. Proposed FacePET System's Software Components

To control the FacePET wearable device and implement the bystanders' consent protocol we developed the following software:

- *FacePET microcontroller's software*: In the current implementation of the FacePET wearable device, this component allows to turn on/off and change the intensity of the goggle's LEDs (in groups of two LEDs independently), and provides a mechanism to control these LEDs from the bystanders' mobile phone via Bluetooth Low Energy (BLE). Since we built the wearable device with the Arduino Uno and the Seedstudio BLE Shield, the RBL_nrf8001 and BLE-SDK Arduino libraries were used to create a Generic Attributes (GATT) BLE server that is used to receive commands from the bystander's mobile phone.
- *FacePET bystander's mobile application*: This application provides the bystander a controller for the FacePET wearable device via BLE to turn on/off and change the intensity of the LEDs, it implements the ACL for the FacePET wearable, and it also implements a Bluetooth protocol that provides the bystander wearing the FacePET wearable device a mechanism to give consent to third-parties who wish to take photos. Initially, the FacePET bystanders' application scans for a FacePET wearable device in the area and once connected to it, it enables the LEDs in the wearable. The LEDs stay powered on until the bystander turn them off, or a third-party FacePET (stranger) mobile application with consent requests a photo to be taken. The protocol to provide consent is described in Section 3.2.3. Figure 7a shows a few screenshots of this mobile application.
- *FacePET third-party (stranger) mobile application*: This application provides a third-party (stranger) a mechanism to ask for consent to take photos from the bystander via Bluetooth. Once consent is given, the application sends a command to the FacePET bystander's mobile application to temporarily disable the FacePET wearable device (as described in Section 3.2.3). Figure 7b shows a few screenshots of this mobile application.

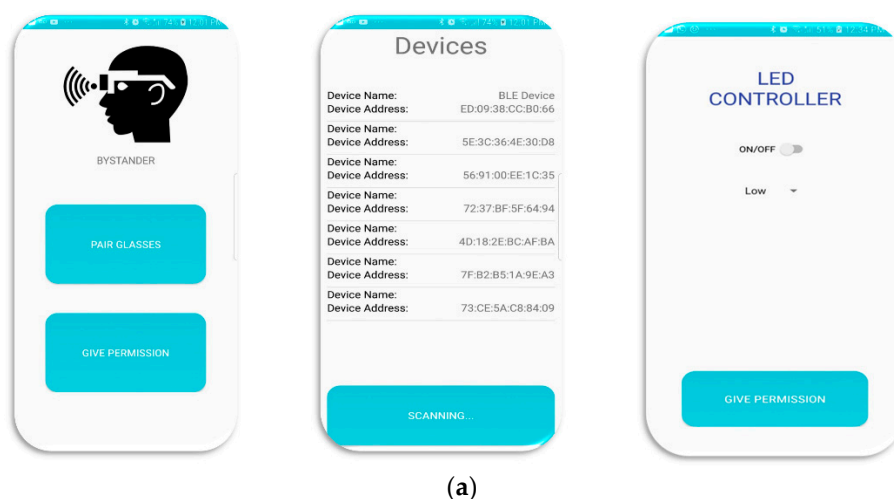


Figure 7. Cont.

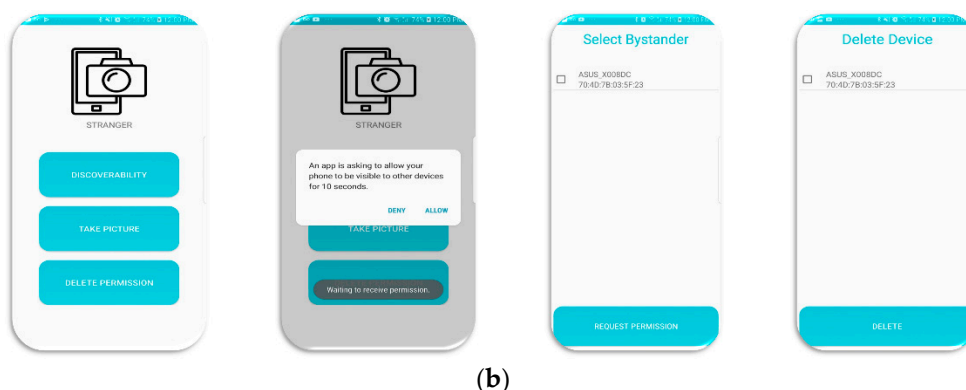


Figure 7. FacePET’s system mobile app screenshots. (a) Bystanders’ application; (b) Stranger (third-party).

3.2.3. FacePET System’s Consent Protocol

As a bystander’s surroundings and context may change over time, he/she may not notice when somebody may take photos of him/her without consent. One of the features and contributions of the FacePET system is the communication protocol that provides a bystander wearing the FacePET device a way to give consent thereby protecting the bystander’s facial privacy and enabling a mechanism to create a list of “trusted cameras” for the bystander.

The protocol (implemented over Bluetooth in our prototype and shown in Figure 8) enables the bystander to control an ACL in the FacePET bystander’s mobile application to enable/disable the FacePET wearable’s LEDs when a trusted third-party mobile phone wants to take photos. Next, we describe a scenario in which three personas, namely Betsy (a bystander using the FacePET system), Trisha (a third-party using the FacePET third-party application) and Steve (a third-party, stranger with a camera) interact at a party.

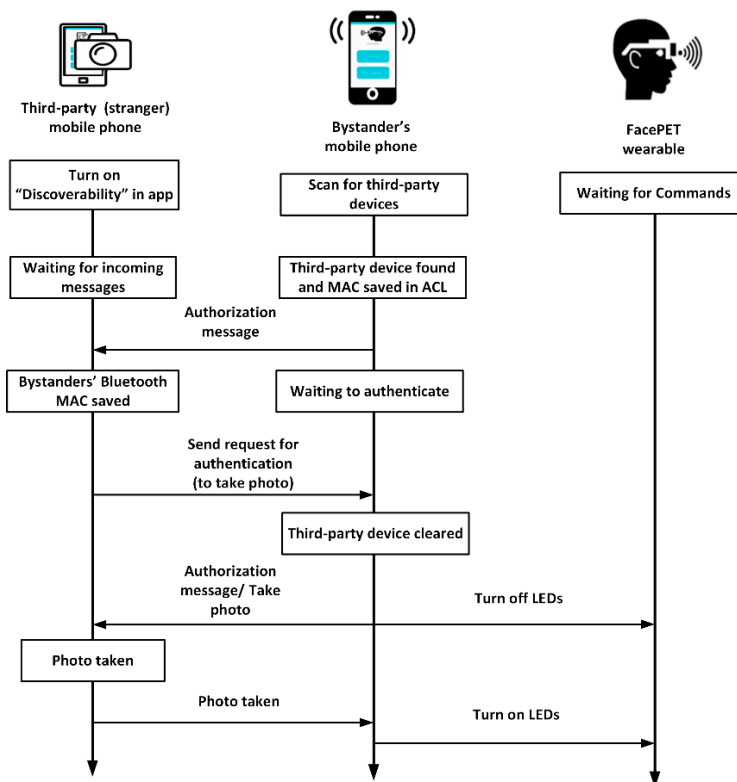


Figure 8. Sequence diagram for FacePET’s consent protocol.

Initially, Betsy is wearing the FacePET system with the LEDs on. Trisha and Besty are friends, and trust each other. Trisha asks Betsy if she can take pictures of her during the party, either by talking to her or through an Internet messaging application (e.g., WhatsApp). If Betsy does not want Trisha to take photos, she simply ignores the message.

However, if Betsy gives consent to Trisha to take photos of her, Betsy replies to Trisha by asking her to open the FacePET third-party (stranger) application and enable the third-party's (stranger) device to be available to be discovered via Bluetooth by the bystander. Then the following steps take place over Bluetooth:

1. Betsy opens the FacePET bystander's mobile application and scans for Bluetooth devices to get Trisha's Bluetooth MAC address and device name.
2. Once Trisha's device is discovered via Bluetooth, Betsy authorizes Trisha's device and the bystander's application saves Trisha's Bluetooth MAC address and device name in a file (Betsy's application adds Trisha's device to the ACL).
3. Betsy's FacePET bystanders' application sends a message via Bluetooth to Trisha's FacePET application notifying that her device is cleared to take photos of Betsy. At this point Betsy's FacePET's application creates a Bluetooth server socket to wait for photo requests from Trisha's FacePET application.
4. Trisha's application saves Betsy's Bluetooth address so that it can be used later to request Betsy's FacePET wearable's LEDs to be turned off (as long both mobile phone devices are in range and Betsy's FacePET mobile application still has Trisha's phone authorized in the ACL).

Later in the party, when Trisha wants to take a photo of Betsy the following steps are followed:

1. Trisha opens her FacePET mobile application. She presses the "Take Photo button" and selects Betsy's device from the list. Trisha's device sends then an authentication message to Betsy's device via Bluetooth.
2. Betsy's FacePET mobile application receives the authentication message. The mobile application then checks if the Trisha's device is authorized in the ACL. If it is, then it notifies Trisha's application that her device can take the photo, and it sends a message via BLE to Besty's FacePET wearable device to turn off the device. Otherwise, Betsy's application ignores the message and the LEDs stay on.
3. Trisha takes the photo and then it sends a message back to Betsy's FacePET's mobile application to turn on the LEDs again.

During the party, Steve (a stranger with camera) has tried to take photos from Betsy's face. Since he does not have permission from Betsy, all the photos he takes from her will look similar to Figure 6c thus protecting Betsy's facial privacy.

With the sensors in the bystander's mobile phone, more complex privacy rules could be created to provide consent. For example, we tested a simple modification wherein a trusted camera can only take a certain number of photos and after the maximum number of authorized photos has been taken by that camera, the FacePET wearable's LEDs will remain powered on. Other contexts may include location, activity or time by modifying FacePET bystander's application to manage the ACL using context-based privacy rules.

4. Evaluation of the FacePET System

We evaluated the effectiveness of the FacePET wearable prototype in protecting facial features by taking photos using digital cameras using different devices (mobile phones and a laptop). These photos were taken using common lighting conditions found in a classroom. We submitted an Institutional Review Board (IRB) application to comply with ethics in research and were approved to perform the experiments. We implemented a Python script that makes use of the OpenCV face detection Application Programming Interface (API) [44]. This script takes as an input a photo file and places a

rectangular square in the photo if it detects a face (as shown in Figure 9a). The OpenCV face detection API provides an open source implementation of the Viola–Jones face detection algorithm trained using 5000 facial and 3000 non-facial images [45].

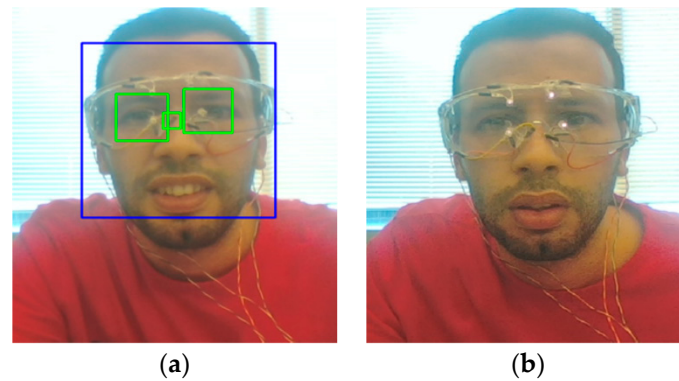


Figure 9. FacePET wearable experiment with IR LEDs. (a) With goggles off; (b) With goggles on. Note that the squares in the left figure and the IR LEDs on the right figure are turned on (LEDS seen as bright white lights between the eyes and around the nasal bone). In the left figure the green and blue squares indicate that a face was detected. In the right figure, the absence of squares indicates that no face was detected.

We initially tested the goggles with IR LEDs by taking a photo with a laptop’s camera and we obtained similar results to those reported by Yamada et al. [18] (Figure 9). Since the laptop’s camera does not have an IR filter, FacePET blocked the Haar-like features. However, when we tested the goggles with IR LEDs using an Apple iPhone 6 (which has an IR filter in the rear-facing camera), the iPhone 6 fully blocked the IR light and allowed the Python script to detect the face. In addition, using IR LEDs to block facial features requires more power when compared to visible light LEDs because most of the energy released from the IR LEDs is perceived as heat. At this point we decided to use visible light and then we tested the goggles using red, green and blue LEDs as shown in Figure 10.

Even though all three type of LEDs block the Haar-like features, we selected the green LEDs as the LED color for the FacePET wearable device because of the widespread use of the Bayer filter [46] in digital cameras which makes these cameras more sensitive to green light wavelengths (to emulate the sensitiveness of the human eye and take photos that are more appealing to humans).

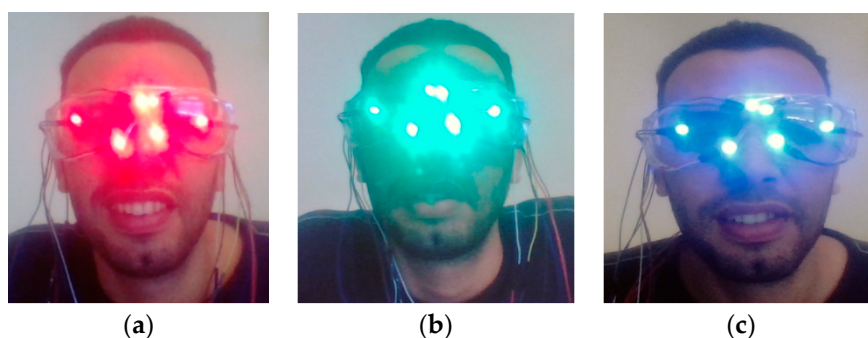


Figure 10. FacePET wearable powered on with different colored LEDs. (a) Red; (b) Green; (c) Blue.

In the next experiment, a user wore the FacePET wearable device in front of different mobile phone’s rear-facing cameras to take photos and later use the OpenCV face detection script that we developed. The goal here was to investigate if the wearable device was effective in protecting a bystander’s facial privacy using the FacePET wearable independently of the camera used. In this experiment green LEDs were used for FacePET. We took photos with 16 different mobile phones as shown in Table 4. OpenCV was able to detect the face only in photos taken with the Samsung

Galaxy 7 and the OnePlus 6 mobile phones (2 out of 16 devices tested, 87.5% of success in blocking OpenCV's Viola–Jones face detection implementation). This shows that using green LEDs for FacePET is effective in protecting a bystander's facial privacy. Finally, we also tested the FacePET's Bluetooth authentication protocol and found that it takes less than 1 s for the third-party app to connect and be authorized by the bystander's application once the third-party device was previously authorized.

Table 4. Results from FacePET facial privacy protection with different rear-facing cameras and OpenCV face detection library. FacePET wearable with green LEDs.

Mobile Phone	Basic Camera Features (Rear Camera; Front Camera; IR Filter)	Face Detected?
Apple iPhone 6 Plus	R: 8 MP; F: 1.2 MP; IR: Yes	No
Apple iPhone 7 Plus	R: 12 MP; F: 7 MP; IR: Yes	No
Apple iPhone 8	R: 12 MP; F: 7 MP; IR: Yes	No
Apple iPhone 8 Plus	R: 12 MP + 12MP (dual cameras); F: 7 MP; IR: Yes	No
Apple iPhone X	R: 12 MP; F: 7 MP; IR: Yes	No
Samsung Galaxy S7	R: 12 MP; F: 5 MP; IR: No	Yes
Samsung Galaxy S7 Edge	R: 12 MP; F: 5 MP; IR: No	No
Samsung Galaxy S8	R: 12 MP; F: 8 MP; IR: No	No
Samsung Galaxy S9	R: 12 MP; F: 8 MP; IR: No	No
Samsung Galaxy S9 Plus	R: 12 MP + 12MP (dual cameras); F: 8 MP; IR: No	No
Samsung Note 7	R: 12 MP; F: 5 MP; IR: No	No
Samsung Note 8	R: 12 MP + 12MP (dual cameras); F: 8 MP; IR: No	No
Asus ZenFone 3 Max	R: 16 MP; F: 8 MP; IR: No	No
Asus ZenFone 4	R: 12 MP + 8MP (dual cameras); F: 8 MP; IR: No	No
OnePlus 6	R: 16 MP + 8MP (dual cameras); F: 16 MP; IR: No	Yes
Motorola Moto G (2nd Gen)	R: 8 MP; F: 2 MP; IR: No	No

Based on the taxonomy presented in Figure 1, the FacePET system belongs to the bystander-based obfuscation category in which the bystanders take actions to avoid their facial identification. In Table 5 we summarize some of the salient differences between our approach and similar ones that have been previously proposed under that category.

Table 5. Salient differences between FacePET and similar methods under the bystander-based obfuscation category. The third column (percentage of successfully blocked/de-identified faces) corresponds to the percentage of blocked/de-identified faces in experiments for each method.

Method	Differences	Percentage of Successfully Blocked/De-Identified Faces
PrivacyVisor [18]	Method uses IR light in goggles and does not work if IR filters used. The method does not allow a bystander to give consent automatically to third parties to take photos to identify the bystander.	100% (assuming a camera without IR filter)
PrivacyVisor III [19]	Method uses visible light through reflective/absorbing material in goggles to block facial features. It does not need power. The method does not allow a bystander to give consent automatically to third parties to take photos to identify the bystander.	Between 90% and 100%
Perturbed eyeglass frames [20]	Method uses patterns in glasses' frames. The prototype was tested as patterns in goggles overlaid over photos. No physical device was developed. This approach is tailored towards face recognition instead of face detection. The method does not allow a bystander to give consent automatically to third parties to take photos to identify the bystander.	80%

Table 5. Cont.

Method	Differences	Percentage of Successfully Blocked/De-Identified Faces
Invisibility Glasses [33]	Method uses IR light in goggles and does not work if IR filters used. This method does not allow a bystander to automatically and selectively allow who can take photos of him or her.	No accuracy reported
FacePET (this work)	Method uses visible light in goggles to block facial features and it also provides the bystander wearing the FacePET a way to give consent automatically to third parties to take photos and identify the bystander.	87.5%

5. Limitations and Future Research

The FacePET device prototype uses visible light to protect and enhance a bystander's facial privacy when the bystander wears the device. This design may be problematic for the wearer and the people surrounding the wearer if a filter is not used to block the light emitted by the FacePET wearable. In our design, we stated that the goggles used in the FacePET wearable should have a filter to block the visible light emitted by the device which is sufficient to avoid eyesight discomfort by a FacePET user. Other people surrounding the device may use a similar approach to avoid discomfort.

To explore the human-computer interaction aspects of the FacePET system, we are conducting a usability study in which we are asking subjects to wear the prototype device and answer questions about its interaction and usability. Even though the complete results of the usability study are beyond the scope of this paper, some of the comments that we have received about the current design are as follows:

- People would ask why the user was wearing such a device.
- The current model is too big and draws attention.
- The model is not stylish.

The feedback gathered through the usability study will open up opportunities to improve the prototype and develop a commercially viable solution to better address the bystanders' facial privacy problem in the future. For example, one improvement to investigate in future FacePET prototypes may include the utilization of smart reflective materials such as the KentOptronics' e-TransFlector™ material [47] that can be directly incorporated on the surface of the goggles and will avoid the utilization of LEDs while at the same time providing a way for the bystander to give consent through the FacePET consent protocol.

In recent years, advances in face detection and recognition techniques and technologies using deep learning methods such as Convolutional Neural Networks (CNN) and Region-based CNNs (RCNNs) [48,49] are outperforming more traditional computer vision methods such as the Viola–Jones approach in accuracy and speed. With these new deep learning approaches our FacePET prototype may not be useful in protecting bystanders' facial privacy. Future work will focus on the development of bystander-based obfuscation/adversarial methods to overcome these new technological advances.

6. Conclusions

We have described the design and implementation of the FacePET system, a wearable/IoT system to enhance bystanders' facial privacy by providing a method for bystanders to protect and provide consent. FacePET enables the bystander to thwart the Viola–Jones face detection algorithm used in computer vision by hiding the Haar-like features required by this algorithm with visible light (green LEDs in our wearable prototype). To the best of our knowledge, this is the first work that investigates and describes an IoT device to enhance the privacy of its wearer, therefore opening up new applications for wearables/IoT devices in the realm of privacy.

In the future, we will investigate various aspects related to the usability of the FacePET system, the utilization of alternative methods that do not require LEDs, the optimization of FacePET's power consumption, and the development of adversarial methods to thwart newer facial detection and recognition algorithms based on deep learning methods.

Author Contributions: Conceptualization, A.J.P. and S.Z.; Funding acquisition, A.J.P.; Investigation, L.Y.M.G., J.M. and S.G.; Software, L.Y.M.G. and J.M.; Supervision, A.J.P.; Writing—original draft, A.J.P.; Writing—review & editing, S.Z.

Funding: This research was funded by the U.S. National Science Foundation and the U.S. Department of Defense under grant award no. 1560214.

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.

References

1. The Ericsson Mobility Report. Available online: <https://www.ericsson.com/en/mobility-report> (accessed on 30 August 2018).
2. Perez, A.J.; Zeadally, S.; Griffith, S. Bystanders' Privacy. *IT Prof.* **2017**, *19*, 61–65. [CrossRef]
3. Perez, A.J.; Zeadally, S. Privacy Issues and Solutions for Consumer Wearables. *IT Prof.* **2018**, *20*, 46–56. [CrossRef]
4. This Russian Technology Can Identify You with Just a Picture of Your Face. Available online: <http://www.businessinsider.com/findface-facial-recognition-can-identify-you-with-just-a-picture-of-your-face-2016-6> (accessed on 18 September 2018).
5. Mitchell, R. Sensing mine, yours, theirs, and ours: Interpersonal ubiquitous interactions. In Proceedings of the 2015 ACM Int'l. Symposium Wearable Computers (ISWC 2015), Osaka, Japan, 7–11 September 2015; pp. 933–938.
6. 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 32nd SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 2377–2386.
7. Flammer, I. Genteel Wearables: Bystander-Centered Design. *IEEE Secur. Priv.* **2016**, *14*, 73–79. [CrossRef]
8. Hatuka, T.; Toch, E. Being visible in public space: The normalisation of asymmetrical visibility. *Urban Stud.* **2017**, *54*, 984–998. [CrossRef]
9. Palen, L.; Salzman, M.; Youngs, E. Going wireless: Behavior & practice of new mobile phone users. In Proceedings of the 2000 ACM Conf. on Computer Supported Cooperative Work (CSCW'00), Philadelphia, PA, USA, 2–6 December 2000; pp. 201–210.
10. 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, 26–30 January 2015; pp. 231–244.
11. 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.
12. 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.
13. 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 8,848,059, 30 September 2014.
14. Wagstaff, J. Using Bluetooth to Disable Camera Phones. Available online: http://www.loosewireblog.com/2004/09/using_bluetooth.html (accessed on 21 September 2018).
15. 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.
16. Blank, P.; Kirrane, S.; Spiekermann, S. Privacy-Aware Restricted Areas for Unmanned Aerial Systems. *IEEE Secur. Priv.* **2018**, *16*, 70–79. [CrossRef]

17. 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.
18. 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.
19. 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.
20. 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 Conf. Computer and Communications Security (CCS 2016), Vienna, Austria, 24–28 October 2016; pp. 1528–1540.
21. ObscuraCam: Secure Smart Camera. Available online: <https://guardianproject.info/apps/obscuracam/> (accessed on 30 September 2018).
22. 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.
23. Nielsen, J. *Usability Engineering*, 1st ed.; Academic Press: Cambridge, MA, USA, 1993; ISBN 978-0125184052.
24. Zeadally, S.; Khan, S.; Chilamkurti, N. Energy-efficient Networking: Past, present, and future. *J. Supercomput.* **2012**, *62*, 1093–1118. [[CrossRef](#)]
25. Hjeltnæs, E.; Low, B.K. Face detection: A survey. *Comput. Vis. Image Underst.* **2001**, *83*, 236–274. [[CrossRef](#)]
26. Yang, M.H.; Kriegman, D.J.; Ahuja, N. Detecting faces in images: A survey. *IEEE Trans. Pattern Anal. Mach. Intell.* **2002**, *24*, 34–58. [[CrossRef](#)]
27. Facebook’s Push for Facial Recognition Prompts Privacy Alarms. Available online: <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html> (accessed on 5 October 2018).
28. Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras. Available online: <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> (accessed on 5 October 2018).
29. Face Recognition. Available online: https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-face-recognition.pdf/view (accessed on 5 October 2018).
30. 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.
31. 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.
32. 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.
33. AVG Reveals Invisibility Glasses at Pepcom Barcelona. Available online: <http://now.avg.com/avg-reveals-invisibility-glasses-at-pepcom-barcelona>. (accessed on 30 September 2018).
34. 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 2009 12th International Conference on Computer Vision, Kyoto, Japan, 29 September–2 October 2009; pp. 2373–2380.
35. Li, A.; Li, Q.; Gao, W. Privacycamera: Cooperative privacy-aware photographing with mobile phones. In Proceedings of the 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 27–30 June 2016; pp. 1–9.
36. 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 2007 IEEE/RSJ International Conference on Intelligent Robots and Systems, San Diego, CA, USA, 29 October–2 November 2007; pp. 65–89.
37. 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](#)]

38. 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.
39. 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.
40. Zhang, C.; Zhengyou, Z. *A Survey of Recent Advances in Face Detection*; Microsoft Technical Report; Microsoft Corporation: Redmond, WA, USA, 2010.
41. Viola, P.; Jones, M. Robust real-time face detection. *Int. J. Comput. Vis.* **2004**, *57*, 137–154. [[CrossRef](#)]
42. Arduino Uno Rev3. Available online: <https://store.arduino.cc/usa/arduino-uno-rev3> (accessed on 8 October 2018).
43. Seedstudio Bluetooth Low Energy Shield Version 2.1. Available online: <https://www.seeedstudio.com/Bluetooth-4.0-Low-Energy-BLE-Shield-v2.1-p-1995.html> (accessed on 8 October 2018).
44. Face Detection using Haar Cascades. Available online: https://docs.opencv.org/3.4.2/d7/d8b/tutorial_py_face_detection.html (accessed on 8 October 2018).
45. Lienhart, R.; Kuranov, A.; Pisarevsky, V. Empirical analysis of detection cascades of boosted classifiers for rapid object detection. In Proceedings of the Joint Pattern Recognition Symposium, Magdeburg, Germany, 10–12 September 2003; pp. 297–304.
46. Bayer, B.E. Color Imaging Array. U.S. Patent 3,971,065, 20 July 1976.
47. KentOptronics e-TransFlector™. Available online: <http://www.kentoptronics.com/solutions.html> (accessed on 19 November 2018).
48. Sun, X.; Wu, P.; Hoi, S.C. Face detection using deep learning: An improved faster RCNN approach. *Neurocomputing* **2018**, *299*, 42–50. [[CrossRef](#)]
49. Ren, S.; He, K.; Girshick, R.; Sun, J. Faster R-CNN: Towards real-time object detection with region proposal networks. In Proceedings of the Neural Information Processing Systems Conference, Montreal, QC, Canada, 7–12 December 2015; pp. 91–99.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).