2-2019

Design and Evaluation of a Wearable System for Facial Privacy

Scott Griffith

DESIGN AND EVALUATION OF A WEARABLE SYSTEM FOR FACIAL PRIVACY

Scott Griffith

2019

COLUMBUS STATE UNIVERSITY

The Graduate Program in Applied Computer Science

DESIGN AND EVALUATION OF A WEARABLE SYSTEM FOR FACIAL PRIVACY

A THESIS SUBMITTED TO

TSYS SCHOOL OF COMPUTER SCIENCE

IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

BY

SCOTT GRIFFITH

COLUMBUS, GEORGIA

2019

DESIGN AND EVALUATION OF A WEARABLE SYSTEM FOR FACIAL PRIVACY

By

Scott Griffith

Committee Chair:

Dr. Alfredo Perez

Committee Members:

Dr. Yesem Peker

Dr. Lydia Ray

Dr. Shamim Khan

Columbus State University

February 2019

ABSTRACT

Through the increasingly common use of devices that provide ubiquitous sensor data such as wearables, mobile phones, and Internet-connected devices of the sort, privacy challenges are becoming even more significant. One major challenge that requires more focus is bystanders' privacy, as there are too few solutions that solve the issue. Of the solutions available, many of them do not give bystanders a choice in how their private data is used. Bystanders' privacy has become an afterthought when it comes to data capture in the forms of photographs, videos, voice recordings, etc. and continues to remain that way. This thesis provides a solution to enhance bystanders' facial privacy by developing a wearable device called FacePET that provides a way for bystanders to protect their privacy and give consent. FacePET was evaluated using experiments to detect faces in photos when users wore the device and by performing a usability study with 21 participants. We found that FacePET was successfully able to block 15 of the 21 participants' faces, yielding a success percentage of 71%. We found through the usability study that a majority of the participants would be willing to use FacePET, or a similar device, daily for their facial privacy protection.

Keywords: Bystanders' privacy; Face detection; Face recognition; Privacy; Wearables; Internet of Things.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

My advisor and committee members: Dr. Alfredo Perez, Dr. Yesem Peker, Dr. Lydia Ray, and Dr. Shamim Khan.

My family.

Chapter 1. Introduction

1.1 Bystanders' Privacy

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. It is worthy to note that this issue arises with any camera-enabled Internet of Things (IoT) device such as web/security cameras and drones.

As an example in which bystanders were identified by using photos of their faces without consent, in 2016 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. Examples like this one underscore the risks that people are exposed to with respect to their facial privacy given the technology currently available.

Looking at it from a human-computer interaction standpoint, research in the early 2000s found that cellphone use in public spaces was offensive to some people [5] seeing as they presented a conflict of social spaces where the user occupied both the physical and virtual spaces at the same time. With wearable devices in today's world such as smart glasses also including cameras and microphones, strong privacy concerns are being provoked by the collection and sharing of data over the Internet without permission, thereby directly threatening bystanders' space and autonomy [6].

1.2 Problem Statement

With such a rise in concerns about bystanders' privacy from consumers, there is yet to be a viable solution that allows for bystanders to be more in control. Most research in the past decade or so have been more focused on the privacy of the wearer instead of whoever else's privacy can be affected by the data collection effort. There are several reasons why this issue needs more attention from researchers and the general consumers. For one, consumers lack the means to control their privacy when using wearable devices. Another reason is that bystanders do not want their privacy to be exposed when somebody is using a wearable device nearby. Lastly, no standard approach exists to handle third-parties in consumer wearables. Thus, researchers began developing ways to combat bystander's privacy by various means.

1.3 Our Contribution

We summarize our contributions as follows:

- The design and implementation of a wearable device, called FacePET, that uses LED lights to block a camera's ability to detect faces. The device is geared towards preserving the privacy of whomever is to wear it.
- A consent protocol over Bluetooth that provides users wearing the FacePET a way to give consent.
- A user study on wearable, Internet of Things devices geared towards facial privacy protection.

Thesis Organization

The first chapter of this thesis includes an introduction of what bystanders' privacy is, the problem statement, and what our contribution is to the area of study. The second chapter consists of a general overview of face detection and recognition algorithms, the methods of bystanders' privacy systems, the design issues of those systems, recent protection methods developed by other researchers, and an evaluation of how well the

methods perform. Chapter three provides a description of the wearable system's development which includes detailed explanations of the system's components as well as the roles of each built application and how they work. Chapter four analyzes and discusses the results of the tests done with human participants using the device. Lastly, chapter five concludes this thesis's research and considers recommendations for future work.

Chapter 2. Background

2.1 Introduction

Before getting into our own solution regarding the issue of bystanders' privacy, we must first study the research and solutions others have done that have helped us get to the point we are at now. As we go through this chapter, we will analyze and explain exactly how face detection and recognition work as well as the algorithms that make them possible. We will also present a taxonomy of bystanders' facial privacy solutions, and a review of current methods available in the literature to enhance the facial privacy of bystanders. As a note, the information in this chapter, as well as in Chapter 3, has been published in the *Electronics* journal [41].

2.2 Face Detection and Recognition

Even though research in face detection and recognition dates back from the 1970's [7 – 8], the advent of imaging sensors embedded in smartphones and digital cameras in conjunction with social networks have made research in the development of these algorithms to flourish in the last decade. Private companies (e.g., Facebook [9]) in addition to law enforcement agencies [10 – 11] are using algorithms to detect faces for business and law enforcement purposes. In computer vision and image processing, face detection is the problem of detecting if a face is present in a photo/video and face recognition is the problem of associating a face in a photo/video with an identity.

The processes involved in the detection and recognition of faces in photos and/or video recordings are presented in Figure 1. Initially photos or videos are captured using some type of digital camera embedded in an IoT device such as a mobile phone, a drone, or Internet-connected camera (image capture phase). Then, these digital photos/videos are passed through software that checks if faces are present in the photo/video (face

detection phase). Finally, if faces are detected, then the face recognition phase is performed. The output of this last phase are the identities of the detected faces.

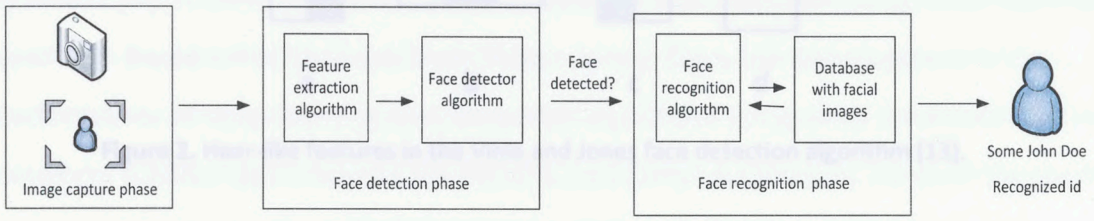

Figure 1. Processes for face detection and recognition.

The development of fast and practical implementations of face detection algorithms in portable devices was possible through the work of Viola – Jones who developed a face detector that became a standard technique for this task [12]. Viola – Jones' work is based on three main ideas [13]: (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 [13]. In the algorithm, a Haar-like feature is calculated as follows [14]:

$$h(r1, r2) = s(r1) - s(r2)$$

where s(r1) is the average of the intensities of the pixels in the "white" regions, and s(r2) 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 2.

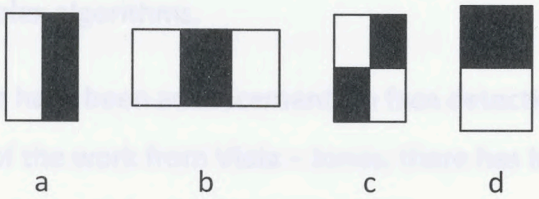

Figure 2. Haar-like features in the Viola and Jones face detection algorithm [13].

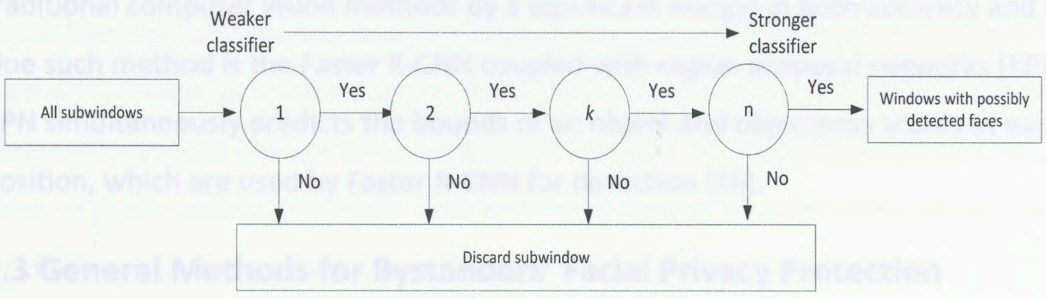

Figure 3. Cascade classifiers in Viola – Jones [12].

The goal on the use of 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 relations between pixels in an image, with more expensive computational cost than the Viola – Jones' approach [12].

The Viola – Jones algorithm calculates the values of these Haar-like features by making use of windows (subregions) 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 have faces in it. The classifier is built as a sequence (cascade) of (weak) classifiers (Figure 3) 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 [13]. Once the windows classified with "yes" have been labeled by the cascade classifier, they may be passed to more complex algorithms.

In recent years, there have been advancements in face detection using deep learning methods. Based off of the work from Viola – Jones, there has been success in the performance of deep learning face detection algorithms using deep convolutional neural networks (CNN), region-based CNN (RCNN), and Faster R-CNN [15]. Most of the recently developed methods stem off of the Faster R-CNN and are often able to outperform traditional computer vision methods by a significant margin in both accuracy and speed. One such method is the Faster R-CNN coupled with region proposal networks (RPN). An RPN simultaneously predicts the bounds of an object and objectness scores at each position, which are used by Faster R-CNN for detection [16].

2.3 General Methods for Bystanders' Facial Privacy Protection

Methods currently available to handle bystanders' facial privacy can fit into two major groups: *location-dependent methods*, which deny third-party devices the opportunity to collect data; and *obfuscation-dependent methods* which prevent bystanders' facial detection and identification. The taxonomy used in this paper to classify the methods to protect bystanders' facial privacy is presented in Figure 4 below.

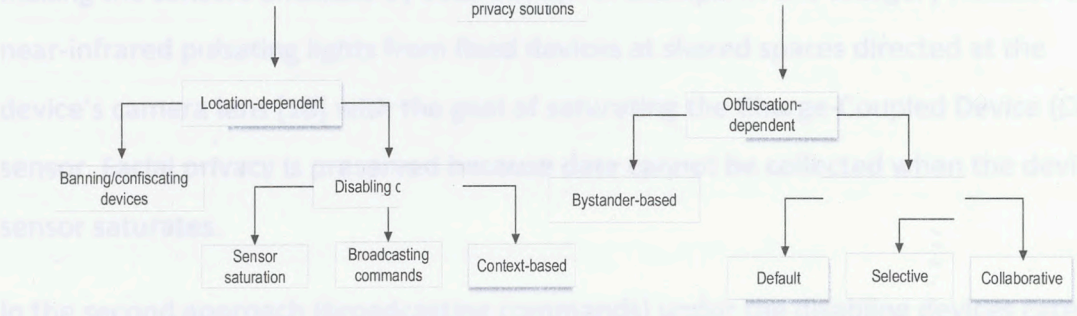

Figure 4. Taxonomy o vstanders' priva

2.3.1 Location-Dependent

The goal of location-dependent methods is to deny the collection of data at particular shared spaces. Implementation of these methods (such as restaurants, casinos, or cafes) 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 4, 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. [17]. As 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 sensors of third-party devices sense 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 includes using near-infrared pulsating lights from fixed devices at shared spaces directed at the device's camera lens [18] with the goal of saturating 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) under the disabling devices category, the third-party devices receive some type of command via wireless communication to disable temporarily the capture of facial data. An example of this category includes the utilization of Bluetooth and infrared protocols to send disabling commands [19 – 20]. In

the last category (context-based approaches) under location-dependent methods, third-party devices perform some type of context recognition to trigger software actions that will deny the explicit collection of data by disabling user devices' sensors at shared spaces.

An example in this category includes the virtual walls approach [21] in which the device uses contextual information (such as 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. [22] 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.

2.3.2 Obfuscation-Dependent

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

In bystander-based obfuscation, bystanders take actions to avoid their facial identification. This might be accomplished by wearing some type of hardware (or clothing) that hides or perturbs 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 [23]. Examples in this category include the PrivacyVisor glasses [14] [24] 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 [25]. Notification methods that alert bystanders to protect their privacy include the use of LEDs on wearables to notify bystanders of video or audio being recorded in their surroundings (such as Snap

spectacles), 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 [23]).

In the last group (device-based obfuscation), the software of 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, blurring all faces detected in a photo or a video), it might let users add noise to obfuscate bystanders selectively (selective obfuscation) [26], 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) [27]. The drawback of device-based obfuscation is that bystanders might have no control on protecting their privacy because device-based obfuscation methods rely on third-party devices for which bystanders have no control.

2.4 Design Issues and Performance Evaluation of Current Methods

Even though solutions to address the issue of bystanders' facial privacy have been proposed in the past (as described in the previous sections), these solutions have issues that depend on the type of method and their implementation. Some of these issues that affect these solutions are as follows:

- Usability: In human-computer interaction, usability is described as how easy a system can be used by a typical consumer/user to fulfill its objectives. In systems to enhance bystanders' facial privacy usable systems should minimize user intervention 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 an issue for these systems.

- 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 contraptions combined with intelligent algorithms. Since these systems make use of artificial intelligence algorithms (i.e., classification algorithms) to detect these contexts and/or faces, these solutions may involve false detections or misclassifications which hinders the effectiveness for the system to work correctly.

Table 1. Design issues for bystanders' facial privacy solutions.

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

Based on these issues, the methods available for bystanders' facial privacy are evaluated by using the ratings for each category as presented in Table 1. The evaluated methods along with their corresponding ratings are described in Table 2 below.

Table 2. Methods for bystanders' facial privacy protection

Method	Category	Usability	Power	Effectiveness	Remarks
BlindSpot Capture-resistant environment [18]	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 [19]	Location	High	Low	Medium	Method requires third-party devices to receive IR commands and software to disable sensors

	(disabling, sensor saturation)				which not all third-party devices may the capability.
Disabling devices via Bluetooth [20]	Location (disabling, sensor saturation)	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 [21]	Location (disabling, sensor saturation)	Moderate	High	Medium	Method requires bystanders to setup privacy rules that are accessed in third-party devices. Use of sensors in mobile device to determine contexts may consume large amounts of power.
Privacy-restricted areas [22]	Location (disabling, sensor saturation)	Moderate	Medium	Medium	Method requires bystanders to setup privacy rules that are accessed in third-party devices. Proposed for unmanned aerial vehicles.
World-driven access control [28]	Location (disabling, sensor saturation)	High	High	Medium	Method does not require bystanders' intervention, but device may not detect contexts correctly.
Sensor Tricorder [29]	Location (disabling, sensor saturation)	High	High	Medium	Method does not require bystanders' intervention, but device may not detect contexts correctly. Makes use of QR codes to encode location privacy rules.
PlaceAvoider [30]	Location (disabling, sensor saturation)	Moderate	High	Medium	Require 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 [23]	Obfuscation-based (bystander-based)	Moderate	Low	Medium	Require third-party devices to notify bystanders about possible privacy violations and have the bystander to take action to protect their facial privacy.
PrivacyVisor [24]	Obfuscation-based (bystander-based)	High	High	Low	Use of IR in wearables worn by bystanders to obfuscate facial features. IR can be blocked using filters.
PrivacyVisor III [14]	Obfuscation-based	High	Low	High	Use of reflective materials in wearables used by bystanders to corrupt photos taken about them.

	(bystander-based)				
Perturbed eyeglass frames [25]	Obfuscation-based (bystander-based)	High	High	Medium	Use of patterns in glasses' frames to confuse facial recognition algorithms. May be prone to reidentification.
Invisibility Glasses [31]	Obfuscation-based (bystander-based)	High	High	Low	Use of IR in wearables worn by bystanders to obfuscate facial features. Need high power and IR can be blocked using IR filters which are available for mobile phones.
Privacy Protection in Google StreetView [32]	Obfuscation-based (bystander-based)	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 [26]	Obfuscation-based (bystander-based)	High	High	Medium	This technology blur faces in photos through a mobile app. Face blurring occurs at the mobile phone and depending of the blurring technique bystanders could be re-identified.
I-pic [27]	Obfuscation-based (bystander-based)	Moderate	High	Medium	Use of protocols between bystander and third-party devices to allow/deny blurring based on privacy rules. Face blurring occur at the mobile phone and depending of the blurring technique bystanders could be re-identified.
PrivacyCamera [33]	Obfuscation-based (bystander-based)	Moderate	High	Medium	Use of protocols between bystander and third-party devices to allow/deny blurring based on privacy rules. Face blurring occur at the mobile phone and depending of the blurring technique bystanders could be re-identified.
Respectful Cameras [34]	Obfuscation-based (bystander-based)	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 [35]	Obfuscation-based (bystander-based)	Moderate	High	Medium	Use of protocols between bystander and third-party devices to allow/deny blurring based on privacy rules. Face blurring occur at the mobile phone and depending of the blurring technique the bystanders could be re-identified.
Invisible Light Beacons [36]	Obfuscation-based	High	High	Low	Bystanders use wearable IR beacons to inform capturing devices of privacy rules. Mobile

	(bystander-based)				devices with IR filters will ignore the signal sent by the beacons.
Negative face blurring [37]	Obfuscation-based (bystander-based)	Moderate	Low	Medium	Once captured and stored, blurring of bystanders' faces occur when photos are presented through social networks using stored privacy rules.

Chapter 3. System Description

3.1 FacePET System

In this section, we describe the Facial Privacy Enhancing Technology (FacePET) system developed in conjunction with NSF REU students, Luis Y. Matos Garcia and Jaouad Mouloud. 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 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 on 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. [24] with the following differences:

- In Yamada's work [24] the authors propose 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 to use visible light is that newer cameras in smart phones (e.g., Apple's iPhone 4 and newer) 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 setup permissions for third-party devices to take photos without the noise (disabling temporally the FacePET wearable), hence creating a "smart" wearable.

- The development of a wireless protocol over Bluetooth that enables communication between the bystander and third-party devices to provide and exchange privacy consents.

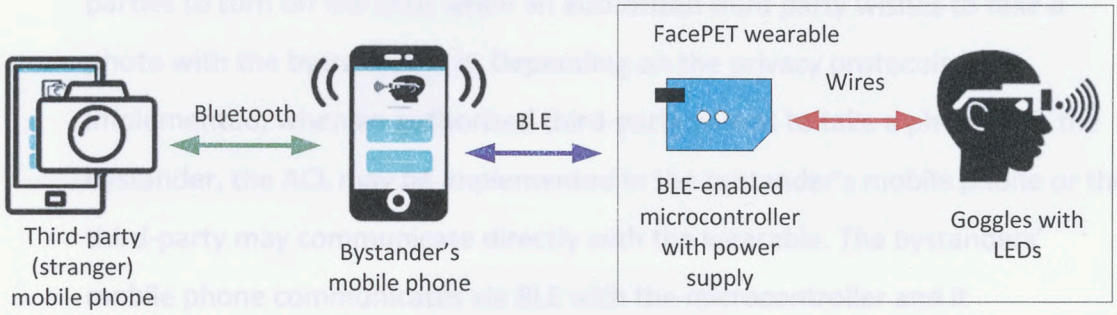

Figure 5. FacePET system's hardware architecture.

3.2 FacePET System's Hardware Architecture

The hardware architecture of the FacePET system (presented in Figure 5) is composed of the following components:

- Goggles with LEDs: The goggles are equipped with LEDs that are turned 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 provides power to them.
- BLE-enabled microcontroller: This component controls the LEDs on the goggles and connects to the bystander's mobile phone via Bluetooth Low Energy (BLE). The microcontroller has its own power supply independent to 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 ACL to disable the LEDs, or the ACL may be implemented at the bystanders' mobile phone software. The FacePET wearable is composed of the BLE microcontroller and the googles (as shown in Figure 5).

- Bystanders' mobile phone: The bystanders' mobile phone executes software that configures the wearable's microcontroller. In addition to configure the wearable, the bystanders' mobile phone executes software that provide 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 communication.
- 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 of the bystander. In our current implementation, these consents are requested via Bluetooth to the bystanders' mobile phone prior to when the third-party can take a photo of the bystander. If consent is given by the bystander, when the third-party mobile phone takes a photo of the bystander, it communicates with the bystander device again to request the LEDs of the goggles to be turned off (if consent has been given previously).

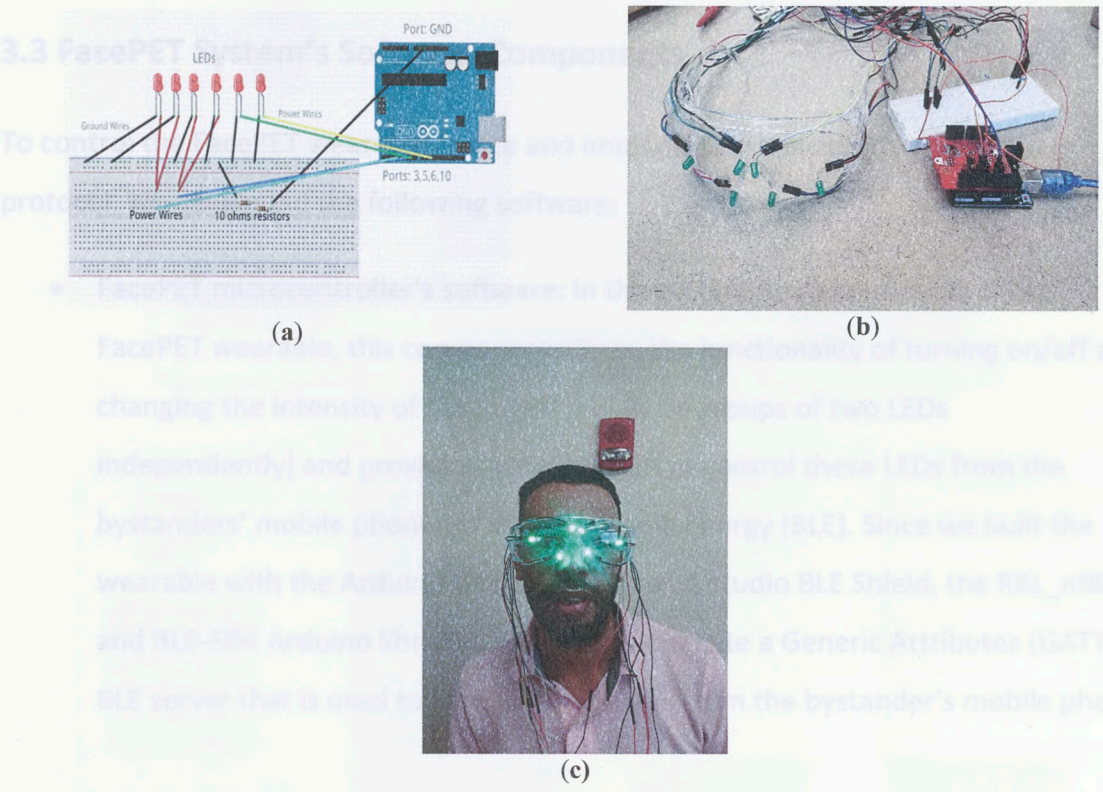

Figure 6. The FacePET wearable device. (**a**) Wiring sketch diagram for FacePET LEDs; (**b**) Goggles with LEDs and BLE microcontroller; (**c**) FacePET wearable prototype worn by a bystander (the person in the photo is Jaouad Mouloud)

In our current prototype we used safety goggles bought at a local hardware store. We placed six LEDs on the goggles as shown in Figure 6(c). 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). As a consequence, we tested red, green and blue LEDs for our prototype. For the BLE-enabled microcontroller in the prototype, we used an Arduino Uno [38] with the Seeed Studio Bluetooth 4.0 Low Energy-BLE Shield v2.1 [39] (Figure 6(b)). The Arduino's power supply used was a battery pack connected to the Arduino's USB-B port. Figure 6(a) shows the wiring sketch diagram for the

Arduino board and the LEDs. We used smartphones that support BLE and can run Android 6 (or better).

3.3 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, this component allows the functionality of turning on/off and changing the intensity of the goggle's LEDs (in groups of two LEDs independently) and providing a mechanism to control these LEDs from the bystanders' mobile phone via Bluetooth Low Energy (BLE). Since we built the wearable with the Arduino Uno and the Seeed Studio BLE Shield, the RBL_nf8001 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.

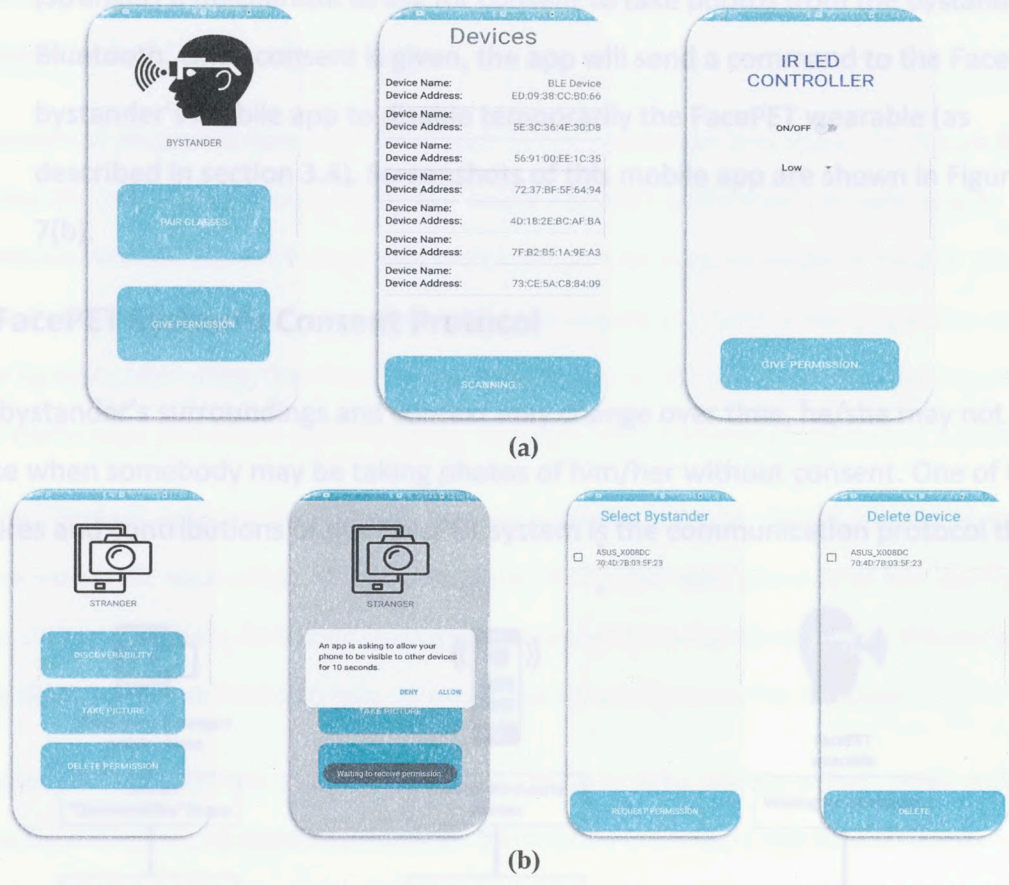

Figure 7. FacePET's system mobile app screenshots. (**a**) Bystanders' app; (**b**) Stranger (third-party)

- FacePET bystander's mobile app: This application provides the bystander a controller for the FacePET wearable 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 to take photos. Initially, the FacePET bystanders' app scans for a FacePET wearable in the area and once connected to it, it enables the LEDs in the wearable. The LEDs stay powered on until the bystander turns them off, or a third-party FacePET (stranger) mobile app with consent requests a photo to be taken. The protocol to provide consent is described in section 3.4. Screenshots of this mobile app are shown in Figure 7(a).

- FacePET third-party (stranger) mobile app: This app provides a third-party (stranger) a mechanism to ask for consent to take photos from the bystander via Bluetooth. Once consent is given, the app will send a command to the FacePET bystander's mobile app to disable temporarily the FacePET wearable (as described in section 3.4). Screenshots of this mobile app are shown in Figure 7(b).

3.4 FacePET System's Consent Protocol

As a bystander's surroundings and context may change over time, he/she may not notice when somebody may be taking photos of him/her without consent. One of the features and contributions of the FacePET system is the communication protocol that

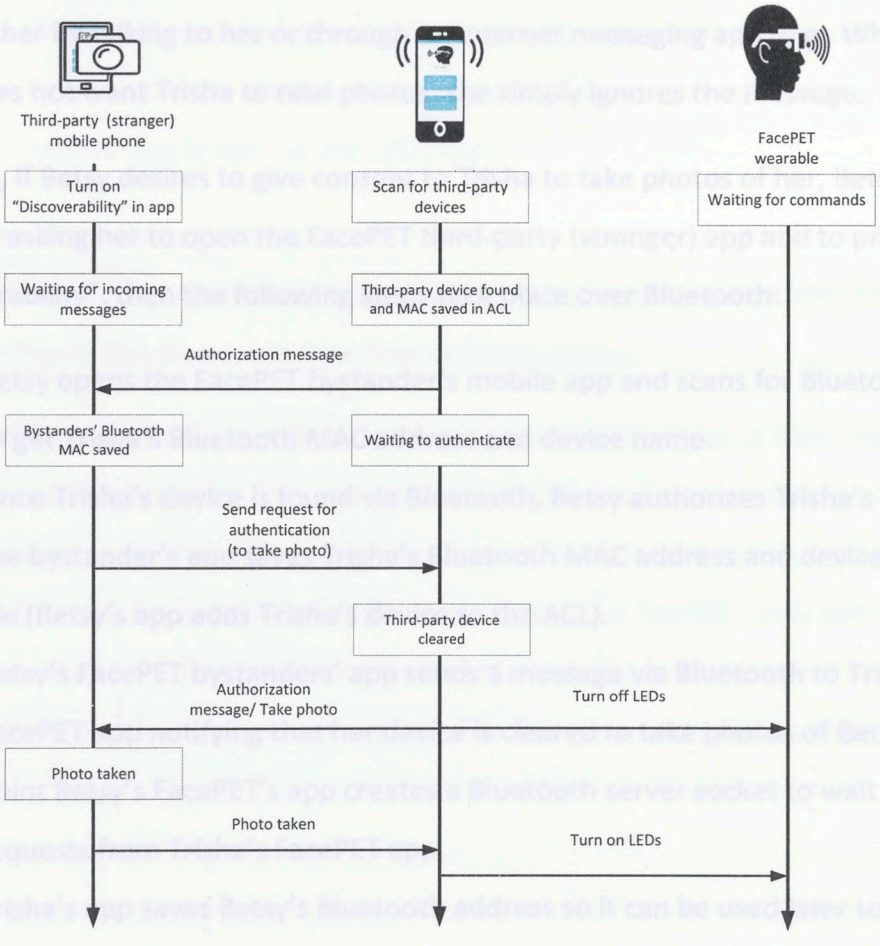

Figure 8. Sequence diagram for FacePET's consent protocol.

provides a bystander wearing the FacePET device a way to give consent, therefore 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 app to enable/disable the FacePET wearable's LEDs when a trusted third-party mobile phone wants to take photos. Now, we will describe a scenario in which three personas, namely Betsy (a bystander using the FacePET system), Trisha (a third-party using the FacePET third-party app) and Steve (a third-party, stranger with a camera) interact at a party.

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 app (e.g., WhatsApp). If Betsy does not want Trisha to take photos, she simply ignores the message.

However, if Betsy desires to give consent to Trisha to take photos of her, Betsy replies to Trisha by asking her to open the FacePET third-party (stranger) app and to press "Discoverability", then the following steps take place over Bluetooth:

1. Betsy opens the FacePET bystander's mobile app and scans for Bluetooth devices to get Trisha's Bluetooth MAC address and device name.
2. Once Trisha's device is found via Bluetooth, Betsy authorizes Trisha's device and the bystander's app saves Trisha's Bluetooth MAC address and device name in a file (Betsy's app adds Trisha's device to the ACL).
3. Betsy's FacePET bystanders' app sends a message via Bluetooth to Trisha's FacePET app notifying that her device is cleared to take photos of Betsy. At this point Betsy's FacePET's app creates a Bluetooth server socket to wait for photo requests from Trisha's FacePET app.
4. Trisha's app saves Betsy's Bluetooth address so 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 app 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 app. She presses the "Take Picture" button and selects Betsy's device from the list. Trisha's device then sends an authentication message to Betsy's device via Bluetooth.
2. The authentication message is received by Betsy's FacePET mobile app. The mobile app then checks if the Trisha's device is authorized in the ACL. If it is, then it notifies back to Trisha's app that her device can take the photo, and it sends a message via BLE to Betsy's FacePET wearable to turn off the device. Otherwise, Betsy's app will ignore the message and the LEDs will stay on.
3. Trisha takes the photo and then it sends a message back to Betsy's FacePET's mobile app to turn on the LEDs again.

During the party, Steve (a stranger with camera) has tried to take photos of Betsy's face. Since he doesn't have permission from Betsy, all the photos he takes from her will look similar to Figure 6(c) 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 in which a trusted camera can take only a certain number of photos and after the max number of photos authorized has been reached for that camera, the FacePET wearable's LEDs will remain powered on. Other contexts may include location, activity or time by modifying the FacePET bystander's app to manage the ACL using context-based privacy rules.

Chapter 4. FacePET Evaluation

4.1 Evaluation Goals

When creating the FacePET wearable device, we had two goals in mind that we wanted to evaluate: usability and effectiveness. For usability, we wanted the interaction between the user and the device to be as easy as possible. For the bystander to setup and work the device as well as control their preferences in the application of who they allow to take their picture should take minimal effort. The same goes for the accompanying application for the stranger and their preference control. As for the effectiveness of the device, the goal was to observe if the wearable device was effective in protecting a bystander's facial privacy using the FacePET wearable independently of the camera being used. The lights around the device are placed in such a way that they hide the Haar-like features of the individual's face well enough to fool face detection algorithms. These two goals were the main focuses of the device going forward into its evaluation.

4.2 Methodology

In order to recruit and collect data from research participants, the necessary Institutional Review Board (IRB) application needed to be filled out and approved. Upon submission, the application was approved on the date of May 14, 2018 and given the approval protocol number 18-108. The initial recruitment of participants was carried out by the supervising professor, Dr. Alfredo J. Perez, who emailed the recruitment flyer to professors in the Computer Science department. The flyer explained that individuals who wanted to take part in the research study were to come to Room 123 in the Synovus Center of Commerce and Technology building on the CSU campus.

Once the participants entered the room, they filled out the informed consent form so that they understood what was taking place. Next, they filled out an initial survey about the general concept of bystanders' privacy as well as their personal preferences on

having their photos taken in certain situations. Then, the participants wore the FacePET wearable device and had their photo taken with the device turned on and off. These photos were then used as input in a Python script that makes use of the OpenCV face detection API [40] which provides an open source implementation of the Viola – Jones face detection algorithm. Lastly, the participants filled out a second survey regarding the wearable device itself and how they felt about it, concluding their participation. A total of 21 participants were surveyed in this study. The results from the study will be presented using tables and graphs in the following section.

4.3 Results

4.3.1 Bystanders' Privacy Survey

The initial bystanders' privacy survey served as a way to gain information about each participant's knowledge of what bystanders' privacy is and how it affects them. Participants were first asked lead-up questions about if they considered themselves a tech savvy person 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. The results to these questions will be discussed later in section 4.4. The participants were then asked to imagine themselves being photographed in certain situations and to choose the privacy action they would be most comfortable with. These results are presented below in Table 3 and in Figure 9.

Table 3. Participants' preferred privacy actions regarding various situations.

Preference when I am...	Preference A) I agree to be captured in any photograph.	Preference B) I agree to be captured, but please send me a copy of any photograph that includes me.	Preference C) Please obscure my appearance in any photograph that includes me.	Preference D) I can decide my preference only after I see the photograph.	Preference E) I do not wish to be captured in any photograph.
At the gym	2	2	0	7	10

Engaging in a daily outdoor activity (e.g. walking cycling, going to market places, etc.)	7	4	5	3	2
In a bar or a nightclub	1	1	4	12	3
At the beach	6	1	2	8	4
At my workplace	9	2	1	7	2
At a place of worship	6	2	1	5	7
Using public transportation	8	0	4	6	3
At a hospital	4	0	3	5	9
In a restaurant	5	3	3	10	0
At a private gathering with family or friends (e.g. birthdays, weddings, etc.)	8	5	1	4	3
At a public gathering (e.g. exhibitions, concerts, movies, etc.)	8	6	3	4	0

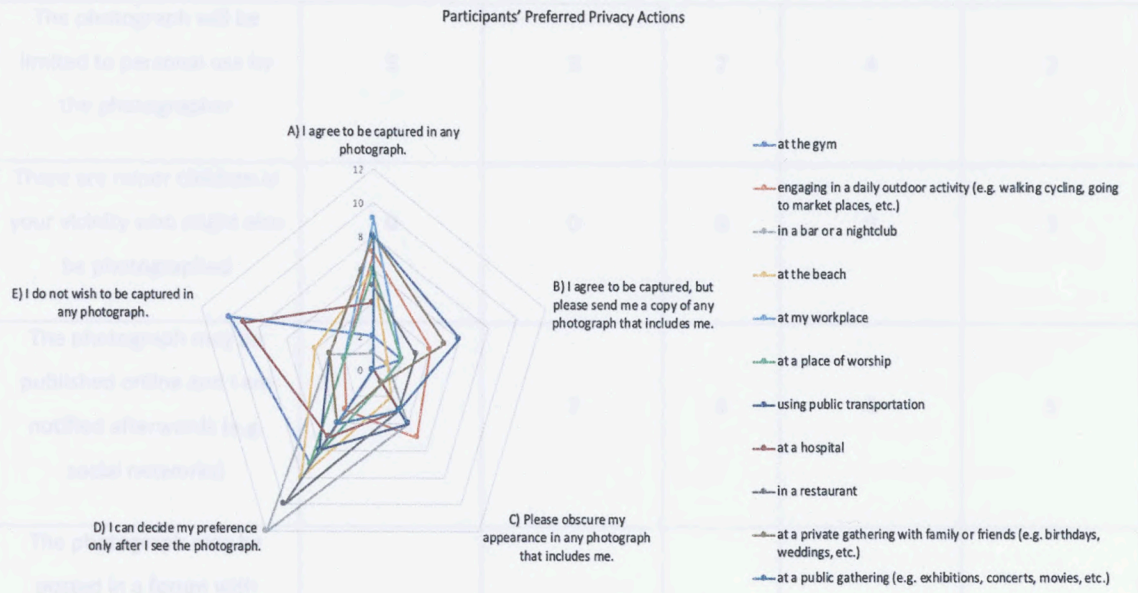

Figure 9. Chart of participants' preferred privacy actions regarding various situations.

After giving their privacy actions for certain situations, the participants were then asked how some given factors would affect their comfort level when being photographed. This was regardless of any specific situation. The results for this part of the survey are shown below in Table 4 and in Figure 10. A final question put the participants in a photographer's position and asked if they would like to respect the privacy preferences of the people around them. These results will be discussed later on as well.

Table 4. Participants' comfort levels regarding various factors.

Comfort when...	Choice A) I will feel much more comfortable	Choice B) I will feel a bit more comfortable	Choice C) I will feel the same	Choice D) I will feel a little less comfortable	Choice E) I will feel much less comfortable
The photographer is a professional photographer (e.g. wedding photographer, journalist, artist, etc.)	13	4	4	0	0

The photograph will be limited to personal use by the photographer	5	3	7	4	2
There are minor children in your vicinity who might also be photographed	0	0	9	9	3
The photograph may be published online and I am notified afterwards (e.g. social networks)	2	2	6	6	5
The photograph may be posted in a forum with restricted membership (e.g. company/university mailing list)	4	4	8	3	2
The photographer is an acquaintance	9	7	5	0	0
The photographer is a stranger	0	0	7	7	7
I am photographed while I am with strangers	0	0	13	3	5
I am photographed while I am with acquaintances	5	8	6	2	0
The photograph may be published online without my knowledge (e.g. social networks)	0	1	4	5	11

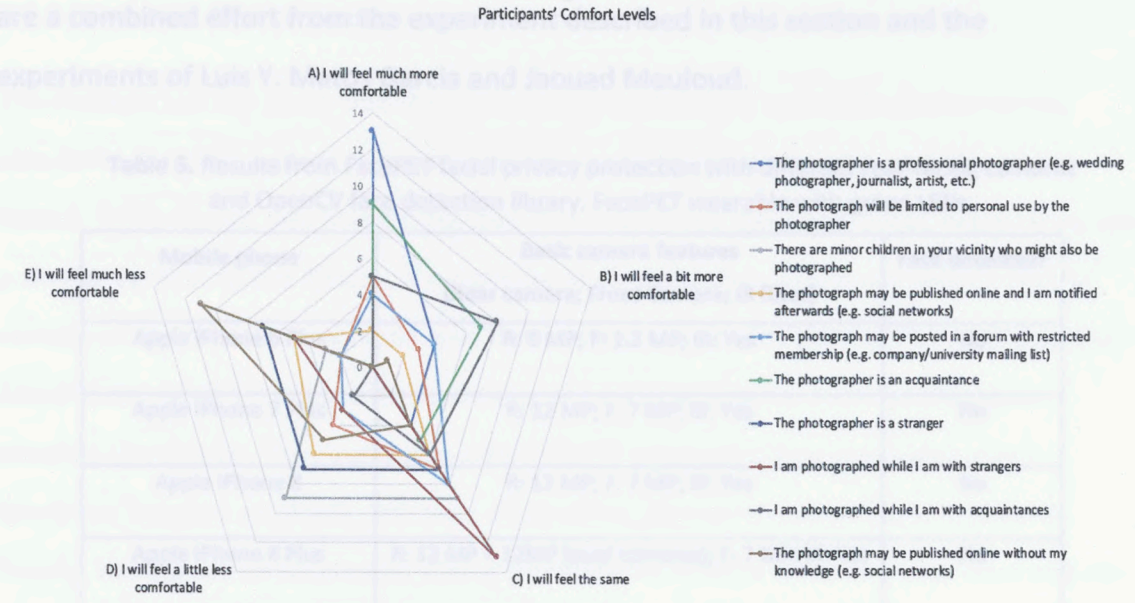

Figure 10. Chart of participants' comfort levels regarding various factors.

4.3.2 Wearing the FacePET System

After participants were finished with the bystanders' privacy survey, they wore the FacePET system and were explained to in detail how the Bystander and Stranger applications worked. Each individual was photographed using the rear-facing camera of an Apple iPhone 7 mobile phone with the device's lights turned on and off, and those photos were used as input in the OpenCV face detection script to show how the device could effectively hide the Haar-like features used in the face detection algorithm. Out of the 21 tests done when taking pictures with the device's lights on, 6 of the participants' faces were still partially or completely detected by OpenCV. This gives a success percentage of 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. For the entire experiment, green LEDs were used for FacePET. The results for face detections using different mobile phones are presented in Table 5 and

are a combined effort from the experiment described in this section and the experiments of Luis Y. Matos Garcia and Jaouad Mouloud.

Table 5. 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: 5 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 (2^{nd} Gen)	R: 8 MP; F: 2 MP; IR: No	No

4.3.3 Wearable Device Survey

The final part of the study had the participants complete a wearable device survey about the FacePET system. It questioned the participants about the usability of the device, if the device was something that they would use daily and if not, would they use a similar version of the device. If a participant decided they would not wear a similar version of the device, they could give their reasons as to why that is. The next question asked them what they think the reactions of people would be when seeing them wearing the device. They were also asked that if wearables that concealed users' identities became available, will they allow smart glasses to become more popular. Finally, the survey concluded by asking participants if there were any improvements to the FacePET system that they would recommend. Results to these questions will also be discussed in the next section.

4.4 Discussion of Results

4.4.1 Bystanders' Privacy Survey Discussion

The first set of questions in the bystanders' privacy survey were able to give insight into participants' practices and knowledge with regards to technology and bystanders' privacy. Out of the 21 total participants, 19 of them considered themselves to be tech savvy while 2 of them thought not so much. When asked how often they took pictures, videos, etc., 3 participants said very often, 4 said pretty often, 4 said often, 8 said not so often, and 2 said very little. The participants were then asked specifically about the issue of bystanders' privacy and how much they knew of it. Surprisingly, most of them did not know much about the issue if anything at all with 2 saying they knew a lot about it, 8 said they knew enough, 8 did not know much, and 3 participants did not even know what it was. In today's world, this issue is more evident than it has ever been, yet most people still do not know it exists. With that aside, most of the participants were in agreement that it is an important issue in today's world with 18 having said it was, and 3 saying it was not.

Moving on to the preferred privacy actions chosen by the participants when in certain situations presented in Table 3 and Figure 9, most of them preferred to either make their decision about the photo after seeing it or they do not wish to be captured in any photo in places such as the gym or in a hospital. In other situations, such as in a bar or nightclub or at a restaurant, most of the participants preferred to make a decision about the photo after seeing it above the other preferences. When at private or public gatherings, the participants are more open to having any photo taken of them, or if a photo is taken then they would want a copy of it. This is understandable since at private gatherings, an individual is surrounded by trusted family and friends, while at public gatherings, such as exhibitions and concerts, almost anyone around will have their phone out taking photos and videos of the event.

Looking at Table 4 and Figure 10, the participants were presented with a new set of questions about how comfortable they would be with different factors affecting them when being photographed. In the presence of a professional photographer or if the photographer was an acquaintance, a majority of the participants chose that they would feel a bit more comfortable if not much more comfortable with having their photo taken. If the factor is that there are minor children in the vicinity who may also be photographed, the photographer is a stranger, or the participant is photographed with strangers, the comfort levels of the participants mainly decreased with them feeling either the same, a bit less comfortable, or much less comfortable. Having minor children captured in photos can be a very sensitive issue depending on varying factors, and when the photographer is a stranger, or an individual is being photographed with strangers, other privacy issues come into play since other people who are not trusted are handling the captured images.

4.4.2 FacePET System Experiment Discussion

It was stated before that of the 21 consecutive pictures taken of the participants' faces, 6 of them were still detected by OpenCV. This is good, but it calls into what factors might be causing almost a third of the faces to be detected. During some of the studies,

it was noticed that the glasses seemed a bit big on some of the participants who had thinner or smaller facial structures. This caused more of the Haar-like features to still be seen through the lenses themselves rather than being blocked in the areas where the LEDs were. There was also an issue with the lighting of the area, where some of the light reflections were mistakenly caught by OpenCV as maybe a glimmer of the eye. Different lighting environments could have a significant effect on the effectiveness of the device.

Analyzing the results from Table 5, it can be seen that OpenCV was able to detect faces only in photos taken with the Samsung Galaxy S7 and the OnePlus 6 mobile phones (2 out of 16 devices tested). This shows that using green LEDs for FacePET is effective in protecting a bystander's facial privacy. Before this experiment, it could be assumed that nicer mobile phone cameras would make it difficult for FacePET to work properly since more detail could be captured. That is certainly not the case seeing as the Apple iPhone 8, iPhone X, and the Samsung Galaxy S9 all came out within the past few years or so and OpenCV still could not detect the faces of individuals.

Regarding the actual uses of the applications for FacePET (the Stranger app in particular), the functionality worked smoothly until the stranger wanted to take a picture. Even when having permission from the bystander to take their picture, the camera would not open up at all on occasion. This could be due to communication errors between the Stranger and Bystander applications, or it could be a software issue which can be fixed.

4.4.3 Wearable Device Survey Discussion

Having had a chance to see how the FacePET system worked, 17 of the 21 participants found the device easy to understand and use, while only 4 found it more difficult. This means that the layout and functionality of the applications was made easy enough for the majority of users to pick up in a small amount of time. When asked if the device was something the participants would use daily, 9 said yes while the other 12 said no. Out of those 12, they were asked if they would use a version similar to FacePET with 7 saying yes and 5 saying no. Even though the original system is not something most of the

participants would use, a majority of them would use a similar version. For those participants who said no to using a similar version of the device, they were asked for reasons as to why with some of the reasons including:

- 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
- Select participants would use a different form of the device, such as a watch

Most of the concerns or reasons surrounding participants not wanting to use the device seem to be because of the devices form factor. Some of the participants who had thinner/smaller facial features found the device sliding down their face, or due to the surface area of the device's lenses compared to some users' faces, most of the identifying facial features could still be picked up by OpenCV as stated previously.

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

- 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

It seems there would be plenty of confusion around the purpose of the device and why anyone would wear it in its current state. Despite the possible reactions to wearing such a device, a majority of the participants did agree that if wearables that conceal users' identities became available, it would allow smart glasses to become more popular with 17 saying yes, 3 feeling indifferent, and only 1 saying no.

To gather some suggestions as to how to improve FacePET, the participants were asked to provide any that they would recommend. Some of the improvements that were repeated among most of the responses included:

- A smaller size of the wearable glasses
- More LEDs to cover more features, or make them less noticeable
- Make the device more fashionable/stylish
- Fix the wiring

The consensus appears to be that FacePET does not match up with the form factor of regular glasses currently available. In order for more people to like wearing the device, they need to look more closely to the types of glasses worn in today's world. This is not to say that some people would not like the current form of the device but changing the style would improve its chances of being popular among consumers.

Chapter 5. Conclusion and Future Work

In this thesis, we have explored deeper into the growing issue surrounding bystanders' privacy by understanding the various algorithms used in face detection as well as evaluating current privacy solutions implemented by researchers over the past years. We were also presented with a description and implementation of the FacePET system which enables the bystander to hide the Haar-like features used by facial detection algorithms by using visible light (green LEDs). Lastly, we analyzed and discussed the results of a study carried out to gain an understanding of individuals' privacy preferences, and to evaluate the FacePET system's usability and effectiveness when used by those individuals. Thanks to this study, we were able to conclude that the majority of the individuals who partook would be willing to wear FacePET, or a similar device, daily for their facial privacy protection, and that if there is an availability of wearables that can conceal users' identities, smart glasses could become more popular.

There is plenty of work to do in the future when it comes to the FacePET system. Plans to improve the system include optimizing its power consumption, changing its form factor in later iterations, and the development of context-based rules that may allow the bystander to setup privacy rules based on location, time and/or activity recognition.

REFERENCES

[1] *Ericsson Mobility Report Q2 Update* [PDF file]. (2018, August). Retrieved from https://www.ericsson.com/assets/local/mobility-report/documents/2018/emr-q2-update-2018.pdf

[2] Perez, A. J., Zeadally, S., & Griffith, S. (2017). Bystanders' Privacy. *IT Professional*, *19*(3), 61-65.

[3] Perez, A. J., & Zeadally, S. (2018). Privacy issues and solutions for consumer wearables. *IT Professional*, *20*(4), 46-56.

[4] Heath, A. (2016, June 22). This Russian technology can identify you with just a picture of your face. Retrieved November 7, 2018, from https://www.businessinsider.com/findface-facial-recognition-can-identify-you-with-just-a-picture-of-your-face-2016-6

[5] Palen, L., Salzman, M., & Youngs, E. (2000, December). Going wireless: behavior & practice of new mobile phone users. In *Proceedings of the 2000 ACM conference on Computer supported cooperative work* (pp. 201-210). ACM.

[6] Motti, V. G., & Caine, K. (2015, January). Users' privacy concerns about wearables. In *International Conference on Financial Cryptography and Data Security* (pp. 231-244). Springer, Berlin, Heidelberg.

[7] Hjelmås, E., & Low, B. K. (2001). Face detection: A survey. *Computer vision and image understanding*, *83*(3), 236-274.

[8] Yang, M. H., Kriegman, D. J., & Ahuja, N. (2002). Detecting faces in images: A survey. *IEEE Transactions on pattern analysis and machine intelligence*, *24*(1), 34-58.

[9] Singer, N. (2018, July 09). Facebook's Push for Facial Recognition Prompts Privacy Alarms. Retrieved November 15, 2018, from https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html

[10] Mozur, P. (2018, July 08). Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras. Retrieved November 15, 2018, from https://www.nytimes.com/2018/07/08/business/china- surveillance-technology.html

[11] Face Recognition. (2013, June 05). Retrieved November 15, 2018, from https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-face-recognition.pdf/view

[12] Zhang, C., & Zhang, Z. (2010). A survey of recent advances in face detection.

[13] Viola, P., & Jones, M. J. (2004). Robust real-time face detection. *International journal of computer vision*, *57*(2), 137-154.

[14] Yamada, T., Gohshi, S., & Echizen, I. (2013, October). Privacy visor: Method based on light absorbing and reflecting properties for preventing face image detection. In *Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on* (pp. 1572-1577). IEEE.

[15] Sun, X., Wu, P., & Hoi, S. C. (2018). Face detection using deep learning: An improved faster RCNN approach. *Neurocomputing*, *299*, 42-50.

[16] Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster r-cnn: Towards real-time object detection with region proposal networks. In *Advances in neural information processing systems* (pp. 91-99).

[17] Jarvis, J. (2011). *Public parts: How sharing in the digital age improves the way we work and live*. Simon and Schuster.

[18] Truong, K. N., Patel, S. N., Summet, J. W., & Abowd, G. D. (2005, September). Preventing camera recording by designing a capture-resistant environment. In *International Conference on Ubiquitous Computing* (pp. 73-86). Springer, Berlin, Heidelberg.

[19] Tiscareno, V., Johnson, K., & Lawrence, C. (2014). *U.S. Patent No. 8,848,059*. Washington, DC: U.S. Patent and Trademark Office.

[20] Wagstaff, J. (2011, November 24). Using Bluetooth To Disable Camera Phones. Retrieved November 15, 2018, from http://www.loosewireblog.com/2004/09/using_bluetooth.html

[21] Kapadia, A., Henderson, T., Fielding, J. J., & Kotz, D. (2007, May). Virtual walls: Protecting digital privacy in pervasive environments. In *International Conference on Pervasive Computing* (pp. 162-179). Springer, Berlin, Heidelberg.

[22] Blank, P., Kirrane, S., & Spiekermann, S. (2018). Privacy-Aware Restricted Areas for Unmanned Aerial Systems. *IEEE Security & Privacy*, *16*(2), 70-79.

[23] Pidcock, S., Smits, R., Hengartner, U., & Goldberg, I. (2011). Notisense: An urban sensing notification system to improve bystander privacy. *PhoneSense*.

[24] Yamada, T., Gohshi, S., & Echizen, I. (2012, October). Use of invisible noise signals to prevent privacy invasion through face recognition from camera images. In *Proceedings of the 20th ACM international conference on Multimedia* (pp. 1315-1316). ACM.

[25] Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016, October). Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1528-1540). ACM.

[26] ObscuraCam: Secure Smart Camera. Retrieved from https://guardianproject.info/apps/obscuracam/

[27] Aditya, P., Sen, R., Druschel, P., Joon Oh, S., Benenson, R., Fritz, M., ... & Wu, T. T. (2016, June). I-pic: A platform for privacy-compliant image capture. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services* (pp. 235-248). ACM.

[28] Roesner, F., Molnar, D., Moshchuk, A., Kohno, T., & Wang, H. J. (2014, November). World-driven access control for continuous sensing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1169-1181). ACM.

[29] Maganis, G., Jung, J., Kohno, T., Sheth, A., & Wetherall, D. (2011, March). Sensor Tricorder: What does that sensor know about me?. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications* (pp. 98-103). ACM.

[30] Templeman, R., Korayem, M., Crandall, D. J., & Kapadia, A. (2014, February). PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces. In *NDSS* (pp. 23-26).

[31] (2015, March 1). Retrieved November 15, 2018, from http://now.avg.com/avg-reveals-invisibility-glasses-at-pepcom-barcelona

[32] Frome, A., Cheung, G., Abdulkader, A., Zennaro, M., Wu, B., Bissacco, A., ... & Vincent, L. (2009, September). Large-scale privacy protection in Google Street View. In *ICCV* (pp. 2373-2380).

[33] Li, A., Li, Q., & Gao, W. (2016, June). Privacycamera: Cooperative privacy-aware photographing with mobile phones. In *Sensing, Communication, and Networking (SECON), 2016 13th Annual IEEE International Conference on* (pp. 1-9). IEEE.

[34] Schiff, J., Meingast, M., Mulligan, D. K., Sastry, S., & Goldberg, K. (2009). Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In *Protecting Privacy in Video Surveillance* (pp. 65-89). Springer, London.

[35] Ra, M. R., Lee, S., Miluzzo, E., & Zavesky, E. (2017). Do Not Capture: Automated Obscurity for Pervasive Imaging. *IEEE Internet Computing*, *21*(3), 82-87.

[36] Ashok, A., Nguyen, V., Gruteser, M., Mandayam, N., Yuan, W., & Dana, K. (2014, September). 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* (pp. 39-44). ACM.

[37] Ye, T., Moynagh, B., Albatal, R., & Gurrin, C. (2014, November). Negative faceblurring: A privacy-by-design approach to visual lifelogging with google glass. In *Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management* (pp. 2036-2038). ACM.

[38] Retrieved from https://store.arduino.cc/usa/arduino-uno-rev3

[39] Bluetooth 4.0 Low Energy-BLE Shield v2.1. Retrieved from https://www.seeedstudio.com/Bluetooth-4.0-Low-Energy-BLE-Shield-v2.1-p-1995.html

[40] Retrieved from https://docs.opencv.org/3.4.2/d7/d8b/tutorial_py_face_detection.html

[41] Perez, A., Zeadally, S., Matos Garcia, L., Mouloud, J., & Griffith, S. (2018). FacePET: Enhancing Bystanders' Facial Privacy with Smart Wearables/Internet of Things. *Electronics*, *7*(12), 379. doi:10.3390/electronics7120379

I have submitted this thesis in partial fulfillment of the requirements for the degree of Master of Science

2/11/19 — Date

Scott Griffith — Scott Griffith

We approve of the thesis of Scott Griffith as presented here.

2/7/2019 — Date

Alfredo Perez, Ph. D.
Assistant Professor, Thesis Advisor

2/6/2019 — Date

Dr. Yesem Peker
Associate Professor

2/7/2019 — Date

Lydia Ray, Ph.D.
Associate Professor

2/6/19 — Date

Dr. Shamim Khan
Graduate Program Director

2/10/19 — Date

Wayne Summers, Ph.D.
Distinguished Chairperson
Professor of Computer Science