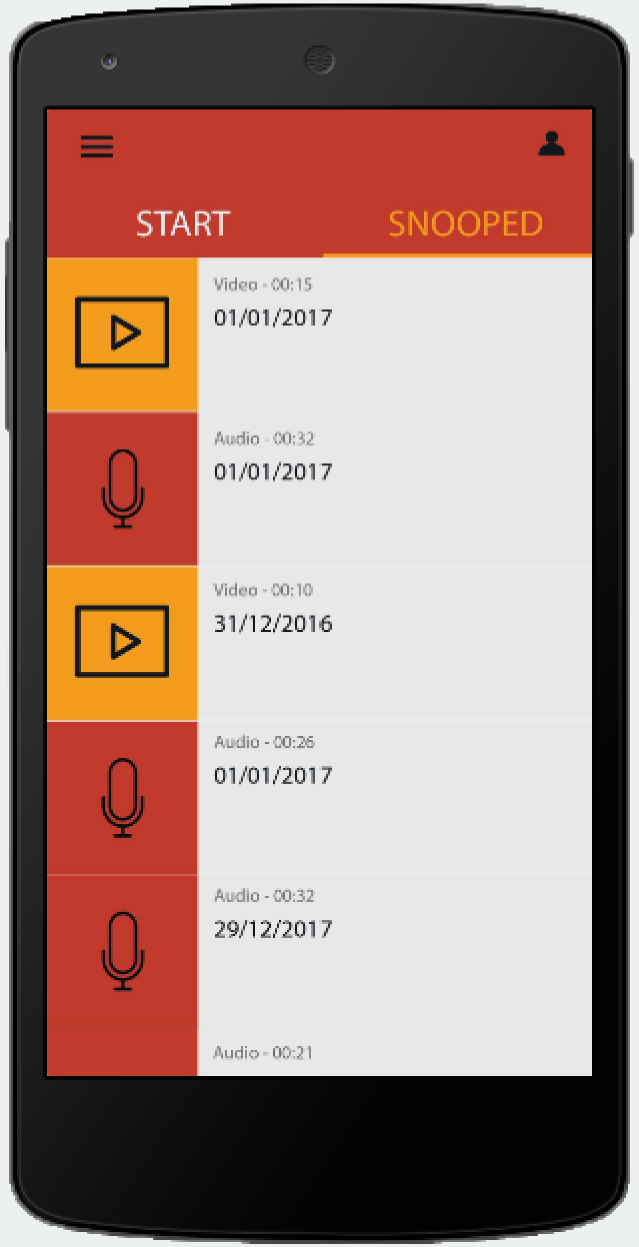
Snoop



Video - 00:15
01/01/2017

Audio - 00:32
01/01/2017

Video - 00:10
31/12/2016

Audio - 00:26
01/01/2017

Audio - 00:32
29/12/2017

Audio - 00:21

Introduction

Overview

As the technologies within our smartphones become increasingly advanced, they increasingly pose a threat to privacy. Companies are incentivized to "datafy" social action, capturing, storing and analyzing more and more individualized data for economic gains (Mayer-Shchonberger, 2013). While governments collect data for national security purposes, hoping to employ the predictive capabilities of Big Data in a process termed "datavaillence" by Van Dijck (2014).

Hackers can also exploit vulnerabilities in code to turn on cameras and microphones in devices without the knowledge of users. Facebook CEO, Mark Zuckerberg, caused a tiny media storm when a picture taken of him showed tape over his laptop camera and microphone jack. In general, however, people don't think of their smartphone cameras and microphones in the same way.

'Snoop' is an Android app which aims to raise awareness of how smartphones can be used to monitor users and collect data about their daily habits and behaviors when certain permissions are enabled in downloaded apps. The app will randomly record video and audio snippets using a smartphone's built in microphones and cameras and store them for later playback. Mobile phones are generally seen as personal devices, with one phone number being attached to one person (Kember and Zylinska, 2012). The app will therefore collect individualized data.

Wider context

How we view privacy is changing (Kitchin, 2014). 'Snoop' will be part of a wider experiment to examine how much we have become conditioned to the idea of giving up our privacy in exchange for goods and services. A subject/subjects will be selected to take part in the experiment and be regularly interviewed for changes in behavior around their smartphone as a result of the app.

Research Questions

5.

How effectively can a smartphone’s microphones and cameras be used as surveillance/datafication devices?

Have we become conditioned to surveillance/datafication?

Is the general perception of privacy and our smartphones in line with recent trends towards surveillance/dataficaion?

How much are people concerned by increasing levels of surveillance/datafication?

Will people's attitudes towards surveillance/datafication change as they are made more aware of the potential for it?

Aim:

To raise awareness of smartphones as potential surveillance and data-collection devices.

Objective 1
Explore solutions to balancing feature-rich devices with user privacy.

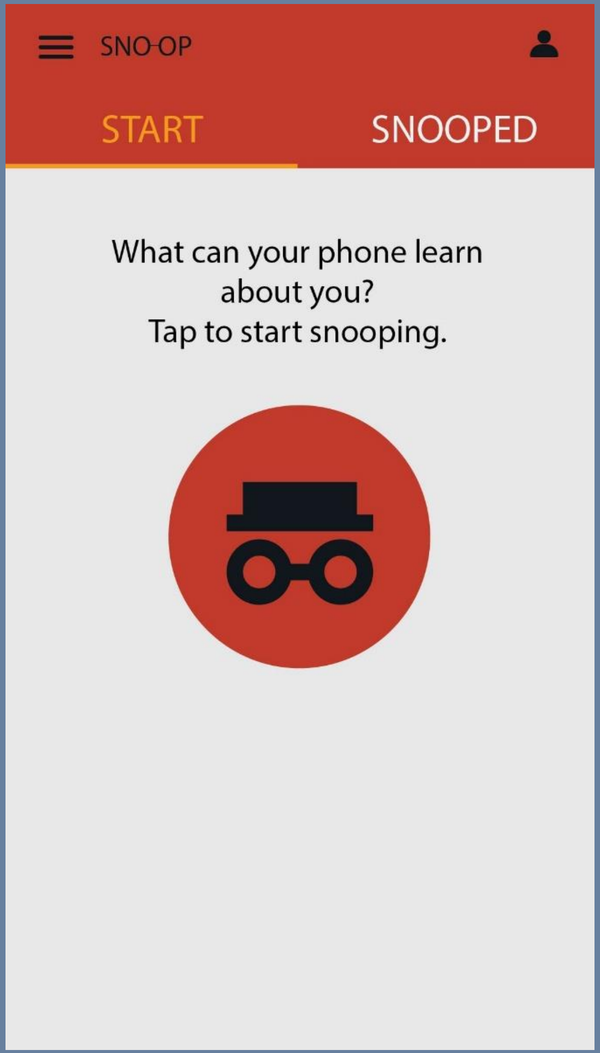
Objective 2:
Examine whether individuals change their behaviour towards their phones when they are aware of being constantly recorded

Objective 3:
Explore today's smartphone users' notions of privacy

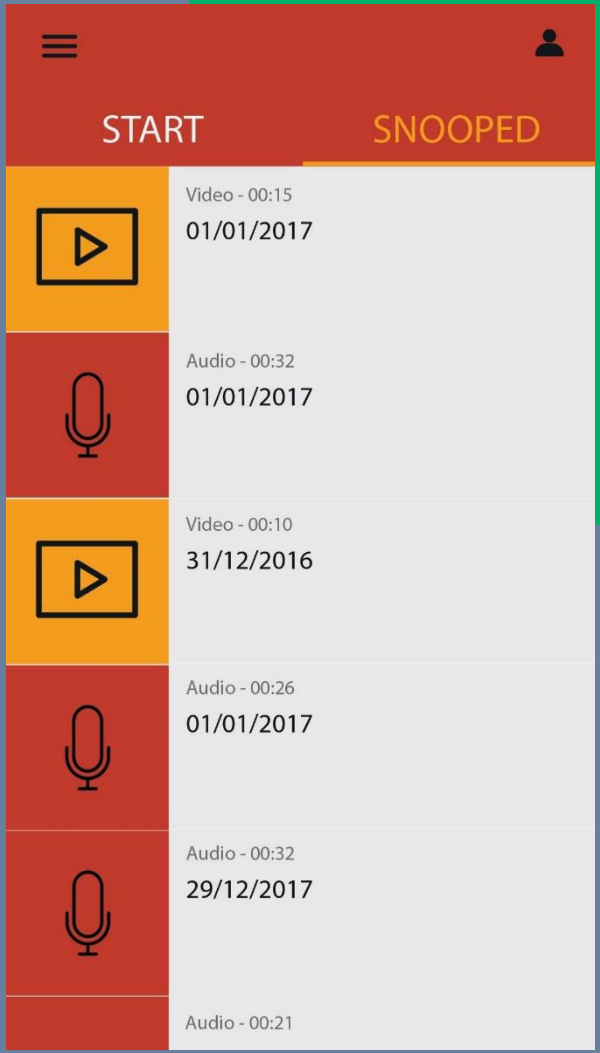
Objective 4:
Explore how much can be found out about an individual's life through randomized monitoring.

Design mock-up

For an interactive version of the app design go to: https://marvelapp.com/3e700e1



What can your phone learn about you?
Tap to start snooping.



Video - 00:15
01/01/2017

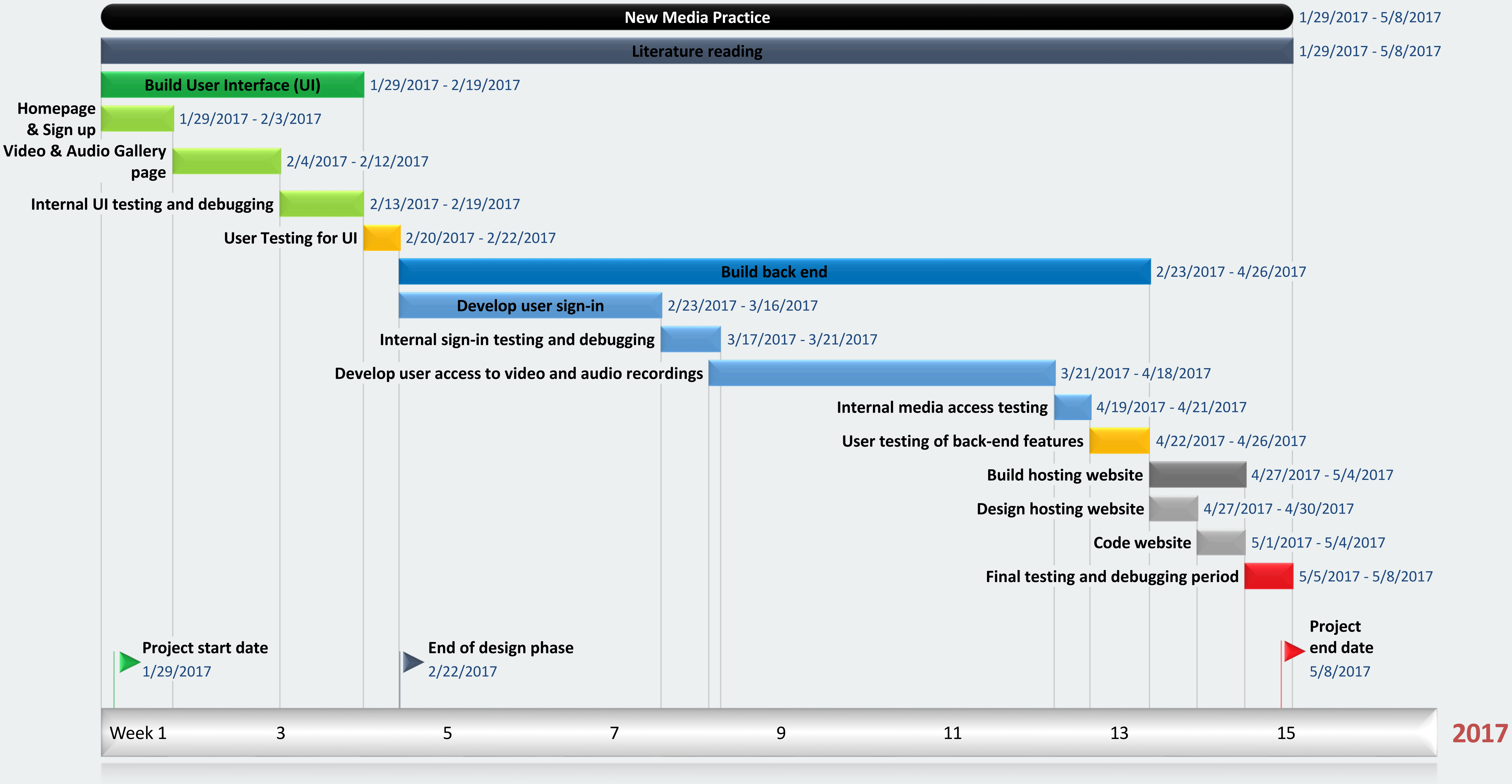
Audio - 00:32
01/01/2017

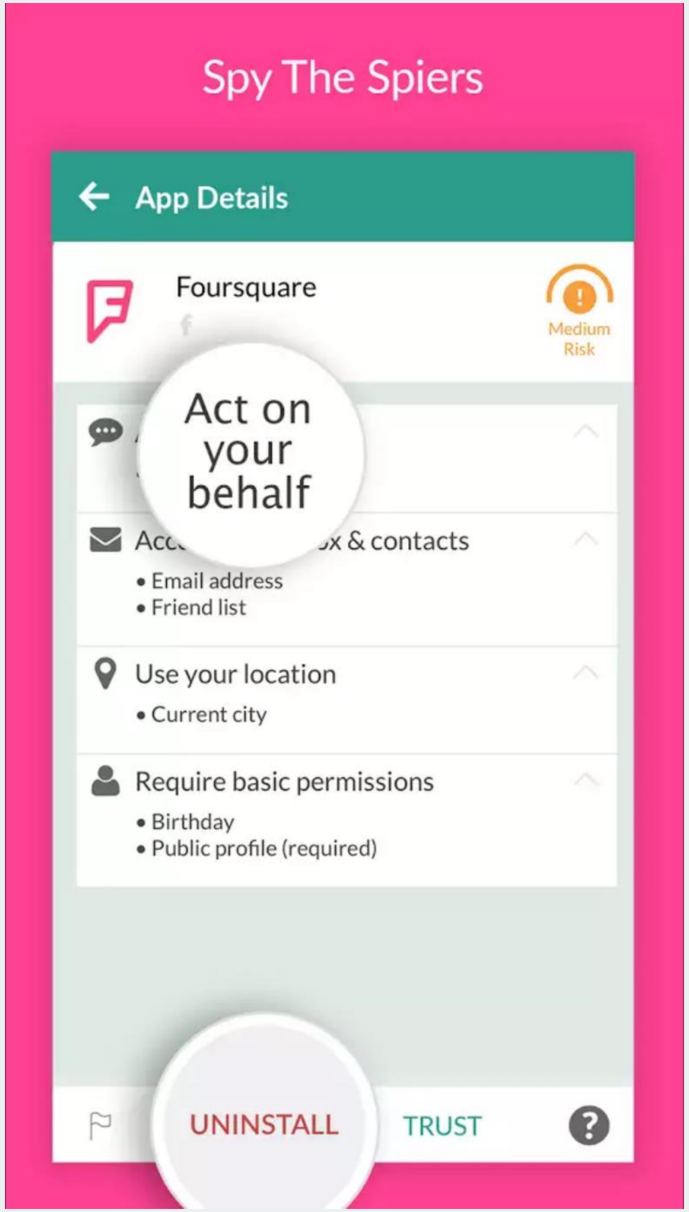
Video - 00:10
31/12/2016

Audio - 00:26
01/01/2017

Audio - 00:32
29/12/2017

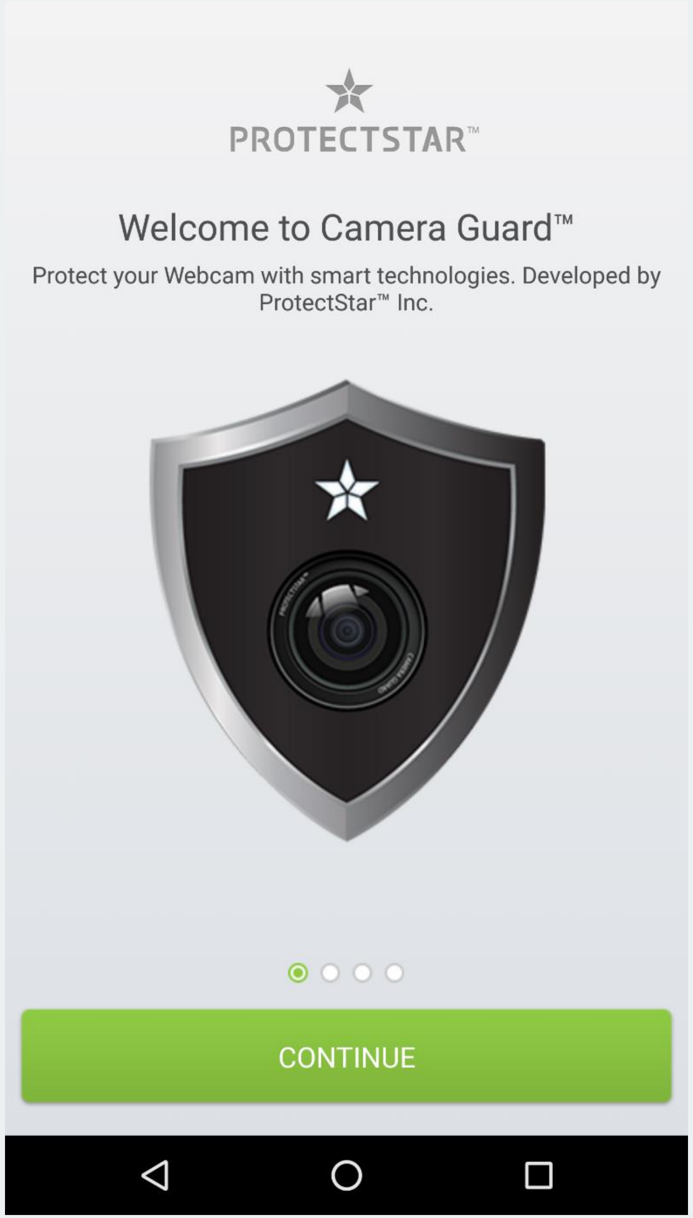
Audio - 00:21


New Media Practice
1/29/2017 - 5/8/2017
Literature reading
1/29/2017 - 5/8/2017
Build User Interface (UI)
1/29/2017 - 2/19/2017
Homepage & Sign up
1/29/2017 - 2/3/2017
Video & Audio Gallery page
2/4/2017 - 2/12/2017
Internal UI testing and debugging
2/13/2017 - 2/19/2017
User Testing for UI
2/20/2017 - 2/22/2017
Build back end
2/23/2017 - 4/26/2017
Develop user sign-in
2/23/2017 - 3/16/2017
Internal sign-in testing and debugging
3/17/2017 - 3/21/2017
Develop user access to video and audio recordings
3/21/2017 - 4/18/2017
Internal media access testing
4/19/2017 - 4/21/2017
User testing of back-end features
4/22/2017 - 4/26/2017
Build hosting website
4/27/2017 - 5/4/2017
Design hosting website
4/27/2017 - 4/30/2017
Code website
5/1/2017 - 5/4/2017
Final testing and debugging period
5/5/2017 - 5/8/2017
Project start date
1/29/2017
End of design phase
2/22/2017
Project end date
5/8/2017
Week 1
3
5
7
9
11
13
15
2017



Related Products

Privacy Cleaner
Privacy Cleaner is an app that scans other apps on your phone and offers a risk profile for each based on the permissions requested. The app ranks apps, with those that it deems to be high risk appearing at the top of its list and those it deems to be low risk appearing at the bottom of its list. Privacy cleaner can help to identify apps that pose a risk to privacy and may help to change behaviour by users around which apps they install and which permissions they grant individual apps. However, it does not demonstrate how these permissions can be misused and may not be able to communicate to users what security permissions actually grant app makers the power to do.

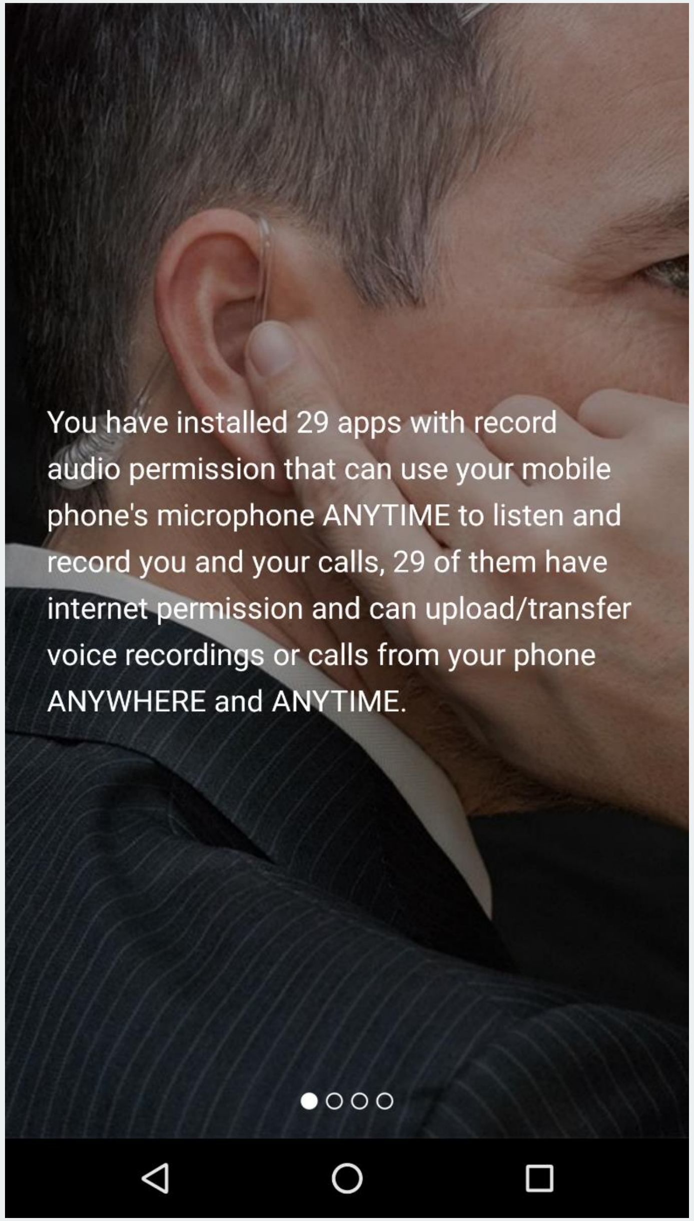


Welcome to Camera Guard™

Protect your Webcam with smart technologies. Developed by ProtectStar™ Inc.

Camera Guard

Camera Guard is an app that blocks other apps installed on the phone from accessing the phone’s camera(s). It analyses each of the apps installed on the phone to see if they already record the user and gives notification each time an app accesses the camera. Using the app could prevent unwanted data from being collected and uploaded unto servers without the user being aware. However, the app does not help to raise awareness about privacy in the way it goes about protecting users from unwanted spying and compromises a key functionality of the phone which is central to popular apps like Snapchat and Instagram.



You have installed 29 apps with record audio permission that can use your mobile phone's microphone ANYTIME to listen and record you and your calls, 29 of them have internet permission and can upload/transfer voice recordings or calls from your phone ANYWHERE and ANYTIME.

Microphone Block

Similar to Camera Guard, Microphone Block is an app that blocks your microphone from being used by other apps and scans your phone for the ones that already record you. Like Camera Guard, the app could potentially prevent unwanted data from being recorded through the use of the microphones but the app has similar failings. Although it allows the user to make calls using the microphone, it blocks a key functionality of the phone to other apps. Apps , like Google Now, use the microphone in its voice recognition technologies.

Bibliography

Kember, S., and Zylinska, J. . 2012. *Life after new media: mediation as a vital process.* [Online]. Cambridge: MIT Presss. Available from: https://www.dawsonera.com/readonline/9780262305358

Kitchin, R. 2014. *The data revolution: big data, open data, data infrastructures and their consequences.* [Online]. London: SAGE. Available from: https://www.vlebooks.com/vleweb/Product/Index/483246?page=0

Mayer-Schönberger, V., and Cukier, K. . 2013. *Big Data: a revolution that will transform how we live, work and think.* London: John Murray.

van Dijck, J. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society.* [Online]. **12**(2), pp.197 - 208. Available from: http://ojs.library.queensu.ca/index.php/surveillance-and-society/index