Project Idea

**Overview**

Our teams project idea is a mobile application, this application will scan the user’s privacy and security settings on Facebook and other social media platforms to allow the user to be more secure and private. The application will work by the user giving us permission to access their social media accounts, once this access has been granted our server side application will analyse the users social media accounts when directed by the user, once the analysis has been completed the mobile application using push requests will notify the user if their account or accounts are in our opinion not secure or as private as they should be. As social media platforms attempt to minimize how much external applications can access or change via their API’s our application will need to use a combination of API calls and web scraping of the user’s profile to accomplish this task.

For example checking a user’s Facebook account using a combination of web scraping and API calls, our application should be able to determine if a user has posts set to public, pictures publicly available besides the required profile and cover photo, has personally identifiable information shared to the public such as employment details, email address, phone numbers, etc., determine what applications have access to their social media accounts which may pose a security or privacy risk and check for chainmail posts.

Users will then be given access to tutorial videos which will be hosted on our own webserver, which will guide them step by step to correct the security and/or privacy concerns our application has found, these concerns will also be explained to the user in simple terms that the non-technical person can understand.

Additionally, the application will also notify the user of privacy agreement and terms of service changes with their social media accounts registered with our application and supplying the user with more insight on how these changes may affect them or others.

Initially the application will be written to target the privacy and security settings of a user’s Facebook accounts, with the long-term goal of also supporting Twitter, Instagram, WeChat, and others in the future.

**Motivation**

The motivation for this application was to empower users of social media to take back control of their online presence and educate them on the security and privacy issues associated with their use of social media.

Humans are social creatures, and the digital era did not change this, but it did vastly change the way we communicate. Using social media, we have instant access to billions of people, and we have new ways of interaction. But social media has privacy and security risks, when not used appropriately. It is used also by criminals for fraud, gathering business intelligence, stealing sensitive information, etc. (Tayouri 2015).

The rise of the social web has traditionally been accompanied by privacy concerns (Netter, Herbst & Pernul 2011). Many people may not be aware of how much personally identifiable information about themselves they are sharing online to the public and how secure their various social media accounts are, or how vulnerable they truly are. How a person has their social media accounts security and privacy settings setup makes a substantial difference in determining how much information about them is available to anyone online and how secure their account is in terms of being vulnerable to hacking or other interference or breaches.

Because we are passionate about privacy and security awareness, we wanted to put users back in control of their social media/digital presence and minimize personal data exposure. We believe this application will be useful in achieving that aim.

**Description**

Application

The project is an application for Android and iOS smartphones that will also require external servers for computational purposes. It will check the security and privacy settings of the user's social media accounts, highlight concerns, and make recommendations to improve the safety of their data and personal information. The user will be given links to tutorials demonstrating how to make changes to their settings and navigate the labyrinth of menus purposely designed in a manor to ensure users share as much data as possible by default to allow the company to achieve maximum monetisation. Notifications will be used as the method of keeping users up to date in changes of company policies that affect security and privacy, so they will continue to be protected over time.

Social Media

The Social Media platform the application will initially support, will be Facebook, with our intended design, we will be able to incorporate more platforms in the future such as Twitter, Snapchat, LinkedIn, Pinterest, and Reddit among many others.

To authenticate these social media accounts, we will be using each platforms API verification methods to conform to their standards for approval.

The security tokens generated by these APIs will then be encrypted and stored on their device by our application and only be decrypted and supplied to our external applications when requested by the user, once the external applications have completed the tasks they will automatically destroy the copy of the token.

If the user were to delete our application these tokens will be deleted by the mobile application after the mobile application revokes its access to their social media platform accounts, ending our access to their social media platform and personal information.

Security, Privacy and Sharing SettingsUsing a combination of web scraping and Facebook API calls we will be reviewing the user’s entire profile from zero day (Account Creation Day), and checking the privacy settings on every post, image, video and flagging chain/spam posts they have shared. And suggesting changes and deletions.

We will also be checking the privacy settings set on individual profile information such as Work and Education, Places Lived, Contact and Basic Information, Family and Relationships, Details about you and life events.

NOTE: These checks will require the users consent each time, As these checks will not be automatic unless the user schedules these checks, scheduled checks will require the users phone to be online with our application running in the background to allow the API tokens to be decrypted and exchanged with our servers otherwise the task will fail.

Additionally, we will use non-invasive reminders for the user not to use the same password on multiple platforms.

Notifications

The application will deliver notifications to the user from our external applications or bulk notifications we have scheduled or if we flag a social media platform as having changed their privacy agreements, terms of service, or other related documents, and data breaches.

Occasionally we will also remind the user to run a privacy check-up if they have not run one in more than 60 days.

Tutorial Videos

Tutorial Videos will be web encoded and streamed using a simple html5 video player.

Each tutorial video will need to be recorded, for both mobile and desktop versions of the website, with closed captions added, long term these will need to be translated closed captions to support additional languages.

Tutorial videos will be predominately screen captures with voice overs.

Innovation

Possible upgrades in the future to the application would be to leverage the power of AI and machine learning to accomplish the web scraping of the social media platforms, allowing the backend applications to adapt easier to layout changes imposed by the individual platforms, this will also vastly reduce development time on a per platform basis.

Limited analytics which are limited in the capacity they can store no personally identifiable information, can be introduced to both the mobile application and backend applications to assist in identifying where users are consistently having issues, for example we would be able to know if users are finding particular tutorial videos difficult to follow and giving up, this information would assist us in creating better tutorials. We would also be able to identify what the most common security and privacy issues are on various platforms and publish this information.

With the use of limited analytics and machine learning the effectiveness of our application will hopefully grow at an exponential rate with the user basis and becoming more effective over time.

**Tools and Technologies**

Our project will be requiring several technologies, tools, and resources to accomplish our project goal. These will be hosted virtual servers, devices for testing our application, software packages, software development kits, and application programming interface documentation.

Virtual Servers

Virtual servers will be used for the backend applications that will be processing the user’s Security, Privacy and Sharing Settings using a combination of API calls and web scraping that will be too complex for a mobile device to accomplish with any real speed.

Some of these will be used as webservers to host various tutorial videos and support pages, we have chosen to use NGINX as our webserver software due to its ability to serve larger visitor numbers than Apache2.

A combination of PostgreSQL and MongoDB database servers will be used by both webpage content and backend application data storage.

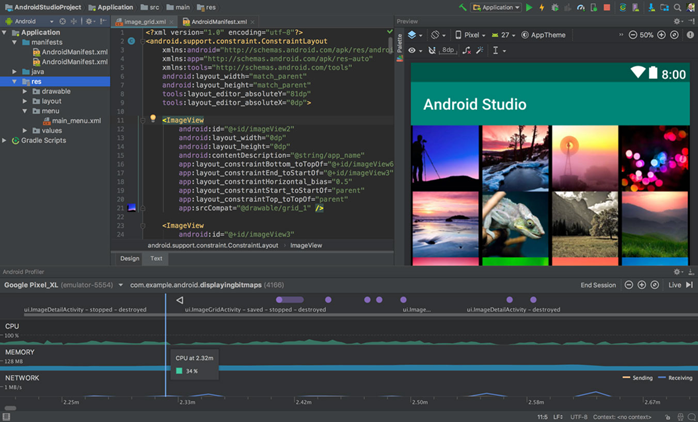
AWS will also be used for end point delivery to the mobile application and for inbound feeds from the social media platforms to avoid security protection systems in place that may block our access as suspicious activity due to the high volume of traffic.

Devices & Testing Platforms

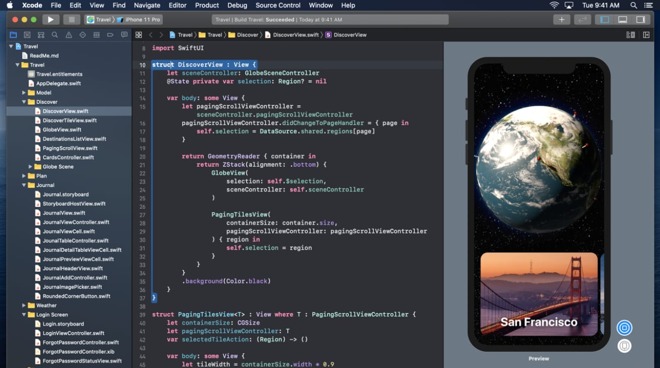
To adequately test our application, we will need access to both a compatible Android device and a compatible Apple device. However, in the early stages of development we can use the development environment SDKs virtual machines to test the basic functionality and review the design of the application.

Development Environment

Android Application - Android Studio will be used to build the mobile application for android devices using the publicly available Android SDK, this software is available on Windows, Mac, Linux, and Chrome OS.



iOS Application – Xcode will be required to build an iOS application and the iOS SDK, unfortunately this is only available on Mac, to get around the hassle of requiring an apple computer we will build a virtual machine running MacOS. This is called a Hackintosh.



Facebook Platform – to access all the features of the Facebook API and SDK we will need a Facebook developer account which is subject to approval and has a complicated and lengthy process.

Code Repository – All code will be checked in private repository’s on GitHub, They will be private to prevent public access to our source code which may benefit a competitor, hackers, or make it easier for social media platforms to prevent us running our various checks.

Backend Development – a combination of PHP, Java and Python will be used to create the various Security, Privacy and Sharing Setting checks, as parts of these checks will be easier to accomplish using different programming languages and will allow us to use a lot of prebuilt software tools.

Tutorial Video Environment  
Open Broadcast Studio, will be used to record our tutorial videos as it allows us to screen capture, and record audio, Adobe Premiere will then be used to edit the footage and insert various extra footage that may be required in the tutorial.

**Skills Required**

* PHP, Python, JAVA
* SQL
* Linux Administration / Management
* Video Editing
* UI Design
* Photo Editing

**Outcome**

If our project is successful, the users of our application will have their social media security and privacy settings aligned with their own personal preference and be only sharing what information they deem fit to the appropriate audiences.

Users will be confident that their use of social media is as safe and secure as their social media provider allows and be aware their accounts are as safe as possible from interference and their data and personal information is secure and protected. Hopefully, users will be educated in the risks associated with social media use and the appropriate settings and measures to take place to mitigate those risks, allowing them to enjoy the benefits of social media and avoid the numerous pitfalls.

With our application monitoring for changes that social media platforms may make to any security or privacy practices or practices, users will also be protected into the future and have no need to be anxious about any adverse changes going unnoticed.

The original problem of poor social media security and privacy will be solved, and user's awareness and education will be improved.

The potential drawbacks are the need to have the application running in the background to allow it to provide notifications about setting changes and possibly the need for the application to be updated periodically.

As the application may not be able to make all the changes to a user’s social media account or accounts itself due to the limitations imposed by the social media platforms to their APIs and will have to rely on the user successfully following tutorials, human error may mean some changes may not actually take affect but the user will think they have, lolling them into a false sense of security, however in this case the application will notify the user again, the user may give up making the changes if the task is too laborious or complicated which it sometimes can be when navigating social media security settings - they aren’t always the easiest to locate.

Another potential obstacle we anticipate is keeping up with the changes in a timely manner and having new tutorial videos ready. The tutorial videos must also be easy to follow and aimed at novices which will need testing - the videos could seem easy to follow to ourselves who have IT experience, but we may leave some people behind. We will keep this in mind during development to make sure the app is effective. With appropriate measures and safeguards we believe this application has the potential to make a real difference in improving social media security and privacy, so it can be used safely and be the enjoyable experience it set out to be without the risk.

**References**

Netter, M, Herbst, S & Pernul, G 'Analyzing Privacy in Social Networks – An Interdisciplinary Approach', 9-11 Oct. 2011, pp. 1327-1334.

Tayouri, D 2015, 'The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages', *Procedia Manufacturing*, vol. 3, pp. 1096-1100.