Skynet-Zuckerberg-Edition

Alexa Aikens, Caroline Arens, Sean May, Sasha Price

CYBR 4580-8950 IA Capstone Project Fall 2020

University of Nebraska at Omaha

Milestone 3: Final Project Milestone

Project Realization Progress Report

Milestone-3.md

Final Report: Packaging and Release

Executive Summary

Training an artificial intelligence to better understand the world through the images that it sees is clearly of interest to Facebook's overall business model. "Yann LeCun (director of FAIR "Facebook AI Research") says that he's confident Facebook's facial recognition is the best in the world, and that it's a key difference between Facebook and academic research institutions. Now, DeepFace is driving force behind Facebook's automatic photo tagging" (Gershgorn). Artificial intelligence-based or AI-based systems like robots and assistants are becoming more and more prominent as the digital landscape continues to expand. As artificial intelligence frameworks are additionally incorporated into crucial parts of society such as mainstream social media applications, any and/or all software applications utilizing an AI-based system such a facial recognition, speaks to the rising curiousity of data privacy with the possibility of affecting the personal security of end users. Facebook specifically has been increasing their footprint in this area. From complex AI algorithm's to extracting data from our images to utilizing artificial neural networks to auto-tag people in photos, Facebook's dedicated engineers intend to create the artificial intelligence of the future. Our goal is to test and analyze Facebook's open source facial recognition libraries to determine if user information is being mishandled based on how it is being collected. Distinctively, calling attention to the particular use of their facial recognition systems and the data collected from it.

The main objectives that we've outlined include: - Analyzing Facebook's open source facial recognition and AI libraries - Testing the front-end user interface to obtain any bias and implications for privacy - Passive network traffic captures using Postman and Wireshark applications - Training the code algorithms and testing the facial recognition models to draw privacy implications

The merit of accomplishing our project's goals and objectives is to provide clear implications for Facebook's social media use.

Project Goals

- Analyze and test Facebook's open-source facial recognition libraries
- Observing the behavior of Facebook's facial recognition feature
- Utilize the Postman API for HTTP method capture
- Draw conclusions about potential privacy implications

Project Methodology

Based on the articles, we plan on examining and testing the code libraries for data vulnerablities.

Discovery Stage

- To analyze and test the code libraries...

We plan to comb through the deepmask and multipath repositositories. While looking through these repositories, we will be taking short notes over what each file does. This allows us to be more focused on the process and less on the code. Most efforts of documentation will be for the data that is obtained and how it will be obtained. We plan to take notes on the data structure to see how the data is represented. Through this we can analyze the empty shell and see the type of data that is being stored. Also, we are taking notes on the behavior of the AI. By understanding the behavior of the AI, we can see what information is needed to complete its job. This will be done by seeing what functions are used and training that is involved.

- Draw conclusions from how the code functions...

- What dependencies do the facial recognition libraries use?
- Summarize & conclude the results we observed from the algorithms

- By researching what Convolutional Neural Networks (CNNs) are and what ours will looks like...

We can further deduce what exactly Facebook is using user's facial recognition data for. From the information we've gathered, a convolutional neural network is a type of deep learning algorithm. It is a kind of artificial neural network (computing systems that are based on a collection of connected units or nodes called artificial neurons) that employs convolution methodology to extract the features from the input data to increase the number of features. Computer vision neural network deep learning models are used to interpret the content of photos users have posted and decide which to surface in the "on this day" feature. So the models underlying the feature have to interpret images and develop a semantic understanding of what's happening. It does this in part by identifying people and objects in images and interpreting the context around them. The models were trained on more than a billion photos that have been uploaded to Facebook over the years, and they have to score in real time millions of new images uploaded each day. It all comes back to keeping users engaged on the social network. Deep learning has played an important role in Facebook's ability to do so, filling a crucial need in the company's business model.

Implementation Stage

From the information in the discovery phase that we synthesized and summarized to discern the potential privacy and data implications, our implementation plan is being conducted in the following ways:

1. By testing the opt-out option/feature for auto-tagging in photo and videos

Facebook tells its users that they are in charge of either allowing or not allowing Facebook to auto-tag them in their (the users) uploaded photos and videos. From previous cases and articles, Facebook's technology can be used to remotely identify people by name without their knowledge or consent. This means that end users cannot control the technology. The on/off setting is there but Facebook still scans faces in photos even when their facial recognition setting is turned "OFF". So how does our project team aim to prove this? Below are our process steps:

1. Create a new Facebook account or utilize one or multiple of the group members accounts
2. Upload multiple photos and/or videos BEFORE manually turning off the facial recognition option for users
3. Test and see if the auto-tagging feature is present once photos/videos are fully uploaded
4. Discover what information is tagged in the photos/videos and conclude if it is accurate
5. Compare the verbiage from the user data and privacy policy agreements to the data/information collected from the tagging feature
6. Turn off the auto-tagging feature manually through Facebook's user settings
7. Upload new photos/videos AND the same photos/videos from step 2
8. After the photos are fully uploaded, compare the auto-tagged photos to any differences in the opted-out photos/videos; this step will show us if the photos that were uploaded AFTER the opt-out option is selected, are still being recognized and marked with tags that the user can select from instead of being auto-tagged after upload.
9. Conclude from our testing if the opt-out feature is truly "OFF" when a user decides to opt-out from Facebook's facial recognition usage/auto-tagging. To discern this we will be able to infer from the tagging options whether the tags presented are the same from the tags that were presented for auto-tagg: meaning, if the tags are the same for opt-out tags and auto-tags then the software is still scanning regardless if the opt-out feature is chosen or not.

After conducting these series of events, we will be able to conclude whether or not Facebook claims to allow its users to keep the auto-tagging feature turned "OFF" or if behind the scenes they may still be scanning every photo and video through their face-matching photo-tagging software.

2. By observing the packets transmitted by Facebook from their user interface

With the understanding of what information Facebook is allowed to process and store, the next goal is to ensure Facebook is following the standards set in place by their own policies, such as their privacy policy, in regard to image data. However, before any interpretation can be made, the data must first be collected. In order to collect the traffic Facebook's web client transmits, we will be using Wireshark to capture raw packets and Postman to follow and organize HTTP/HTTPS traffic.

To capture the transmitted packets, we will use the following procedure in Wireshark:

1. Begin capturing packets in Wireshark. This will also capture large amounts of superfluous data, but this can be filtered out.
2. Login to Facebook using a new account. This account should not have any associations to previous data (such as using personal accounts) as to avoid any distortion of what information Facebook gathers.
3. Upload a photo to Facebook.

   a. Change the account's profile picture to a different photo.

   b. Post a photo to the account's feed without text.

   c. Post a photo to the account's feed with relevant text, such as a caption.
4. Stop capturing packets in Wireshark, and then gather the relevant traffic and export to a capture file. This file will later be searched for any traffic which contains data that is not explicitly permitted according to our findings from policy and legal research.

3. Training and Testing DeepMask models for efficacy with varying smaple size

We need a linux with a video graphics card. This was the base of creating a Deepmask model to training to examine images given to it and evaluating the efficacy of the results.

1. Install Torch and Deepmask
2. Run Training Script to produce Deepmask model
3. Run the Evaluation script on the Deepmask model

Delivery Stage

- We will compile all of our findings into our Github's project readme document and files

- We will conclude from our discoveries if there are any social media implications for privacy

- We will create a report and presentation on our results from our testing outlined above

Results / Findings

Milestone 1

- **Outcome 1**: Compiled information for a Literature Review and related information. Link
- **Outcome 2**: Created a plan for the semester project.

Milestone 2

- **Outcome 1**: We started by packet capturing the network traffic on Facebook using Wireshark to discern if any user data that should not be obtained from Facebook was harvested. We were able to decrypt the TCP packet information from Wireshark by creating a system environment variable called SSLKEYLOGFILE. This harvests the session keys from a SSL layer then passes the key log file into Wireshark to automatically decrypt the file. That then tells us what is being sent over the network by observing what's in the packet. We acheived the browser data of what the image upload sent to Facebook's servers was and we discovered evidence of a key logger called CavalryLogger, which activates when you click on a 'Like' button. We have not determined if this is legal based on Facebook's regulations but there are implications for user's privacy.

- **Outcome 2**: We have initiated a HTTP method capture in Postman instead that will yield more useful information that is easier to interpret. To collect the input infromation provided by the user to Facebook when uploading images. Here is the HTTP request captured by Postman app on a Facebook upload. Upload Capture.

- **Outcome 3**: We wanted to test the user interface to discern if the auto-tagging feature would provide any insight to misuse behavior or poor accuracy in user media uploads. This included a false auto-tag of not properly tagging a user who has uploaded a photo of themselves along with not tagging that specific user's friends in a photo when uploaded as well. The facial recognition AI will not recognize the faces of animals as a tag. The effort made in these areas has shown to be trivial due to the user interface behavior behaving according to the user's settings. We are still doing extensive testing on the accuracy of this behavior to try to replicate the behavior. Our expectation is that the accuracy of this behavior is due to a bias that Facebook has implemented through their coding algorithms. Certain data inputs (user photo uploads) do not get tagged properly (auto or manually) depending on the object, gender or race, as well as if the user has a brand new account with not enough data points for Facebook's AI to understand yet. Facebook UI Test Documentation Facebook Auto-Tagging Testing

- **Outcome 4**: We achieved the proper way to conduct our environment setup with hopes of testing DeepMask and MultiPath networks.

Milestone 3

- **Outcome 1**: After fully integrating our setup enivornment in Milestone 2, we achieved the training of our coding algorithm, DeepMask, so that we could begin testing the model. We achieved the testing results after 5 days of training took place. The results are linked here: DeepMask Results

- **Outcome 2**: Diagram of what the neural network looks like for DeepMask and MultiPathNet -- Neural Network Diagrams

- **Outcome 3**: We were able to determine what the facial recognition libraries use and the potential privacy implications for that use and summarize and conclude the results we observed from the algorithms.

Install Instructions (if applicable)

Requirements

- WireShark
- Postman
- CUDA Toolkit
- cuDNN
- Torch
- LUA Rocks
- Deepmask and Sharpmask

Installation Instructions

Postman Configuration
WireShark Configuration
Installation Documentation for CUDA Toolkit, cuDNN, Torch, LUA Rocks, and DeepMask & Sharpmask

Getting started

Postman Procedure
Neural Network Procedures

Presentation

Milestone 3 Presentation

Milestone 2: Prototype Deliverable

Testing Procedure

Facebook Testing Procedure Documentation

Facebook UI Test Documentation
Facebook Auto-Tagging Testing
Postman Testing Procedure
Neural Network Testing

Environment Setup

Below is a table including our work environments setup and instructions:

Tooling/Environment	Installation Requirements	Description/Usage	Configuration
Wireshark	**Windows** The minimum Windows version supported is Windows 10, 8.1, Server 2019, Server 2016, Server 2012 R2, and Server 2012. The older operating systems are not supported. **macOS** The minimum macOS version supported is macOS 10.12 and later. **Linux** >- Debian GNU/Linux - FreeBSD - Red Hat Enterprise Linux / CentOS / Fedora	Our usage of Wireshark is intended to capture the passive network traffic when uploading an image to Facebook	WireShark Configuration
Postman	**macOS** The minimum macOS version supported is macOS 10.10 (Yosemite). **Windows** Windows 7 and later are supported, older operating systems are not supported. Windows for ARM devices is possible by using the ia32 binary. **Linux** Distributions supported on Postman* - Ubuntu 12.04 and newer - Fedora 21 - Debian 8 **Interceptor** Interceptor extension version v0.2.26 or later.	Postman will allow us to do HTTP method captures	Postman Configuration for Interceptor
Facebook Open Source Algorithms	**DeepMask** - MAC OS X or Linux - NVIDIA GPU with compute capability 3.5+ - Torch with packages: COCO API, image, tds, cjson, nnx, optim, inn, cutorch, cunn, cudnn **MultiPathNet** - Linux - NVIDIA GPU with compute capability 3.5+	**DeepMask** DeepMask is applied densely to an image and generates a set of object masks, each with a corresponding objectness score **MultiPathNet** MultiPathNet identifies what the object masks are from DeepMask's generated data	Facebook's DeepMask Facebook's MultiPathNet
Unsplash Image Library	None	For testing the trained DeepMask and MultiPath networks	None

Project Realization

Project_Realization.md

Diagrams

Below are our diagrams which show the high-level concepts and detailed flows of our processes:

This diagram provides a high-level overview of how we will conduct our testing for the DeepMask and MultiPathNet algorithms. Testing will begin with creating sets for training algorithms in order to test the accuracy of a network based on its training sample size. These tests will also include a set of images as input for the trained networks. The output of these images will be compared to a control network which has been trained with the standard amount of samples.

This diagram displays the image analysis procedure used for evaluating the outputs of a DeepMask network. This procedure produces a 'pass' or 'fail' result depending on how effective the mask was. The network produces a mask image and a confidence value. We will calculate the difference between an output and its corresponding control output. A case passes when it is within the threshold values used for both confidence and difference.

This diagram shows the overview of evaluating a MultiPathNet output. Our image is passed into a network, and the output is then determined to be a true positive, false positive, true negative, or false negative. These results are collected, and the totals for each category are used to calculate the F1 score.

Additional Info:

Issue Tracking and Planning

Issues Tracking
Kanban Board

Presentation Video

Milestone 2 Presentation

Milestone 1

Executive Project Summary

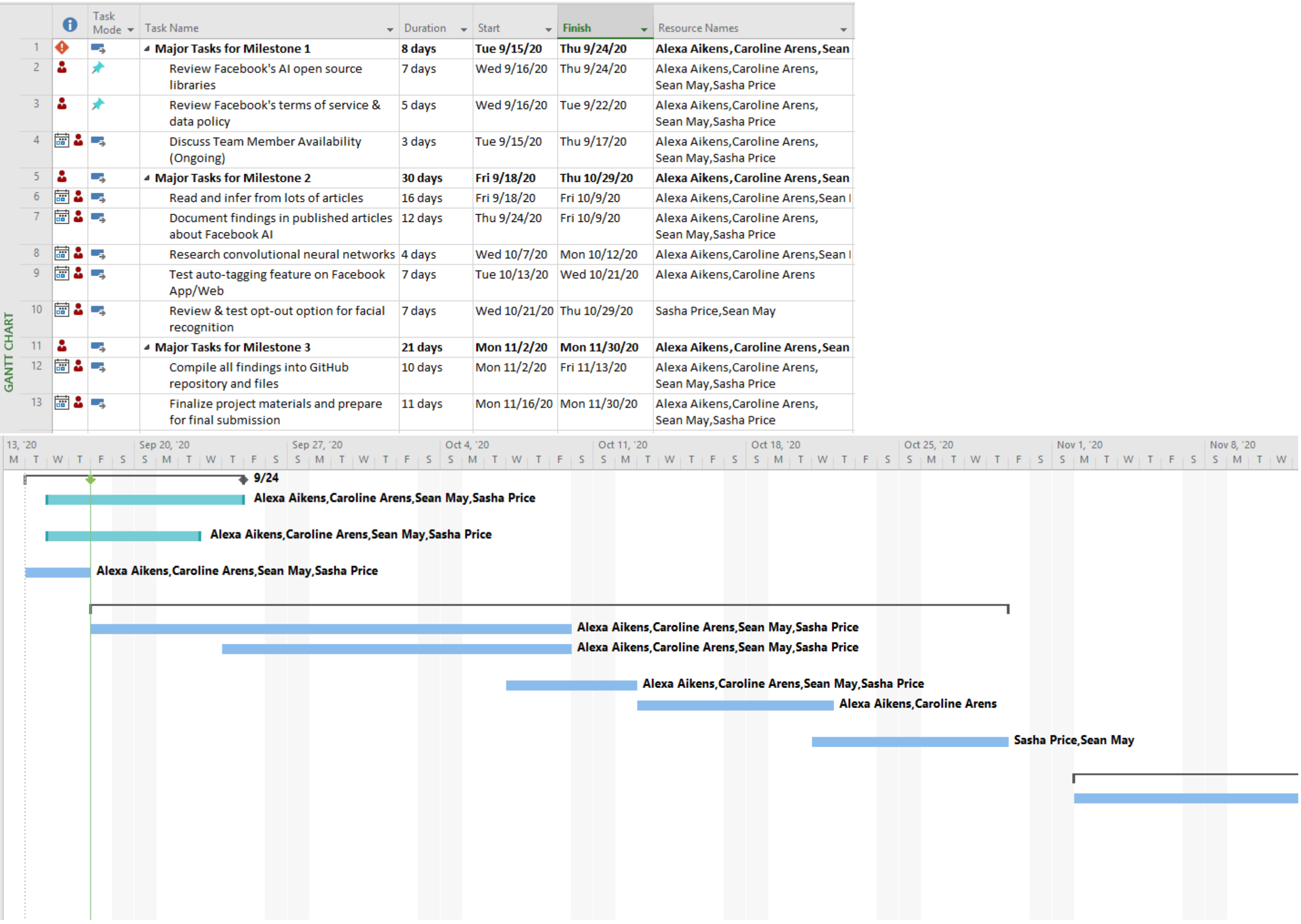
Training an artificial intelligence to better understand the world through the images that it sees is clearly of interest to Facebook's overall business model. "Yann LeCun (director of FAIR "Facebook AI Research") says that he's confident Facebook's facial recognition is the best in the world, and that it's a key difference between Facebook and academic research institutions. Now, DeepFace is driving force behind Facebook's automatic photo tagging" (Gershgorn). Artificial intelligence-based or AI-based systems like robots and assistants are becoming more and more prominent as the digital landscape continues to expand. As artificial intelligence frameworks are additionally incorporated into crucial parts of society such as mainstream social media applications, any and/or all software applications utilizing an AI-based system such a facial recognition, speaks to the rising curiousity of data privacy with the possibility of affecting the personal security of end users. Facebook specifically has been increasing their footprint in this area. From complex AI algorithm's to extracting data from our images to utilizing artificial neural networks to auto-tag people in photos, Facebook's dedicated engineers intend to create the artificial intelligence of the future. Our goal is to test and analyze Facebook's open source facial recognition libraries to determine if user information is being mishandled based on how it is being collected. Distinctively, calling attention to the particular use of their facial recognition systems and the data collected from it.

The main objectives that we've outlined include: - Analyzing Facebook's open source facial recognition and AI libraries - Documenting what information or data is extracted from user videos and images - Determine from the collection of user data, facial or otherwise, is the use of facial recognition a violation of people's privacy by not obtaining appropriate user consent?

The merit of accomplishing our project's goals and objectives is to provide clear implications for social media use. Specifically, Facebook's AI research into facial recognition and how its user policy agreements are not being concise about consent to this.

Proposed Project Timeline

Below is our proposed project timeline. Our Kanban board can be found here: Project Sprint Plan



	ⓘ	Task Mode	Task Name	Duration	Start	Finish	Resource Names
1			**Major Tasks for Milestone 1**	**8 days**	**Tue 9/15/20**	**Thu 9/24/20**	**Alexa Aikens,Caroline Arens,Sean**
2			Review Facebook's AI open source libraries	7 days	Wed 9/16/20	Thu 9/24/20	Alexa Aikens,Caroline Arens, Sean May,Sasha Price
3			Review Facebook's terms of service & data policy	5 days	Wed 9/16/20	Tue 9/22/20	Alexa Aikens,Caroline Arens, Sean May,Sasha Price
4			Discuss Team Member Availability (Ongoing)	3 days	Tue 9/15/20	Thu 9/17/20	Alexa Aikens,Caroline Arens, Sean May,Sasha Price
5			**Major Tasks for Milestone 2**	**30 days**	**Fri 9/18/20**	**Thu 10/29/20**	**Alexa Aikens,Caroline Arens,Sean**
6			Read and infer from lots of articles	16 days	Fri 9/18/20	Fri 10/9/20	Alexa Aikens,Caroline Arens,Sean I
7			Document findings in published articles about Facebook AI	12 days	Thu 9/24/20	Fri 10/9/20	Alexa Aikens,Caroline Arens, Sean May,Sasha Price
8			Research convolutional neural networks	4 days	Wed 10/7/20	Mon 10/12/20	Alexa Aikens,Caroline Arens,Sean I
9			Test auto-tagging feature on Facebook App/Web	7 days	Tue 10/13/20	Wed 10/21/20	Alexa Aikens,Caroline Arens
10			Review & test opt-out option for facial recognition	7 days	Wed 10/21/20	Thu 10/29/20	Sasha Price,Sean May
11			**Major Tasks for Milestone 3**	**21 days**	**Mon 11/2/20**	**Mon 11/30/20**	**Alexa Aikens,Caroline Arens,Sean**
12			Compile all findings into GitHub repository and files	10 days	Mon 11/2/20	Fri 11/13/20	Alexa Aikens,Caroline Arens, Sean May,Sasha Price
13			Finalize project materials and prepare for final submission	11 days	Mon 11/16/20	Mon 11/30/20	Alexa Aikens,Caroline Arens, Sean May,Sasha Price

GANTT CHART
13, '20
Sep 20, '20
Sep 27, '20
Oct 4, '20
Oct 11, '20
Oct 18, '20
Oct 25, '20
Nov 1, '20
Nov 8, '20
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
9/24
Alexa Aikens,Caroline Arens,Sean May,Sasha Price
Alexa Aikens,Caroline Arens,Sean May,Sasha Price
Alexa Aikens,Caroline Arens,Sean May,Sasha Price
Alexa Aikens,Caroline Arens,Sean May,Sasha Price
Alexa Aikens,Caroline Arens,Sean May,Sasha Price
Alexa Aikens,Caroline Arens,Sean May,Sasha Price
Alexa Aikens,Caroline Arens
Sasha Price,Sean May

Project-Oriented Risk List

In our risk list, we have identified the major sources of risk and what we plan to do about them in case they arise.

Risk Name	Impact	Likelihood	Description	Mitigation
Team Member Availability (28)	7	4	Aligning meeting times around academic and work schedules may deem difficult	Plan is to meet each week after weekly check-ins with Dr. Hale until an issue may arise

Risk Name	Impact	Likelihood	Description	Mitigation
Communication/Under communication (24)	8	3	If any requirements are misinterpreted by the project team a gap develops between expectations, requirements and milestones	May need to communicate the same idea many times in different ways before people remember it
Software Availability (27)	9	3	Not all of the necessary software for analysis may be open source	Work around would be to check UNO's available software for students or low cost subscription options
Analysis Complexity (28)	7	4	The scope of the analysis may be very large for our time frame	Focus on AI and facial recognition and its handling specifically instead of all the research of Facebook's AI and data usage
Learning Curves (35)	7	5	Project team may need to acquire new skills for the project so there's a risk that productivity will be low	Try to keep the best member for a certain task doing what they understand best

Literature Review

LitReview
Appendix

Project Methodology

Based on the articles, we plan on examining and testing the code libraries for data vulnerablities.

Discovery Stage

- To analyze the code libraries...

We plan to comb through the deepmask and multipath reposítositories. While looking through these repositories, we will be taking short notes over what each file does. This allows us to be more focused on the process and less on the code. Most efforts of documentation will be for the data that is obtained and how it will be obtained. We plan to take notes on the data structure to see how the data is represented. Through this we can analyze the empty shell and see the type of data that is being stored. Also, we are taking notes on the behavior of the AI. By understanding the behavior of the AI, we can see what information is needed to complete its job. This will be done by seeing what functions are used and training that is involved.

- Data collection of Facebook's Policy on Privacy, Data, and Terms...

For reviewing the Facebook policies, we plan on focusing on the policies that surround Biometric data. This includes how the data is being handled and whether Facebook is recording the data without consent. With focusing on the how the data is being handled, this will allow us to determine whether Facebook is taking the necessary steps to keep the data out of unsecure hands. Also, for the permission to take biometric data, we would want to see if Facebook notifying the users if their data is recorded. We want to know if we have the option to revoke the permission of Facebook recording the data. Finally, the last thing we would like to know, if we delete our accounts will the biometric data be deleted.

- By observing and documenting how the code works and the policies used by Facebook...

For this part we plan to compare the code to the policies we reviewed. We want to see if Facebook has violated its own security policies for biometric data. Through comparing the results, we can also judge whether there needs to be a change in certain policies that do not cover enough, or we can suggest new policies to help cover certain grey areas if they exist.

- By researching what Convolutional Neural Networks (CNNs) are and how they are being used to accomplish Facebook's tasks...

We can further deduce what exactly Facebook is using user's facial recognition data for. From the information we've gathered, a convolutional neural network is a type of deep learning algorithm. It is a kind of artificial neural network (computing systems that are based on a collection of connected units or nodes called artificial neurons) that employs convolution methodology to extract the features from the input data to increase the number of features. Computer vision neural network deep learning models are used to interpret the content of photos users have posted and decide which to surface in the "on this day" feature. So the models underlying the feature have to interpret images and develop a semantic understanding of what's happening. It does this in part by identifying people and objects in images and interpreting the context around them. The models were trained on more than a billion photos that have been uploaded to Facebook over the years, and they have to score in real time millions of new images uploaded each day. It all comes back to keeping users engaged on the social network. Deep learning has played an important role in Facebook's ability to do so, filling a crucial need in the company's business model.

Implementation Stage

From the information in the discovery phase that we synthesized and summarized to discern the potential privacy and data implications, our implementation plan is being conducted in the following ways:

1. By testing the opt-out option/feature for auto-tagging in photo and videos

Facebook tells its users that they are in charge of either allowing or not allowing Facebook to auto-tag them in their (the users) uploaded photos and videos. From previous cases and articles, Facebook's technology can be used to remotely identify people by name without their knowledge or consent. This means that end users cannot control the technology. The on/off setting is there but Facebook still scans faces in photos even when their facial recognition setting is turned "OFF". So how does our project team aim to prove this? Below are our process steps:

1. Create a new Facebook account or utilize one or multiple of the group members accounts
2. Upload multiple photos and/or videos BEFORE manually turning off the facial recognition option for users
3. Test and see if the auto-tagging feature is present once photos/videos are fully uploaded
4. Discover what information is tagged in the photos/videos and conclude if it is accurate
5. Compare the verbiage from the user data and privacy policy agreements to the data/information collected from the tagging feature
6. Turn off the auto-tagging feature manually through Facebook's user settings
7. Upload new photos/videos AND the same photos/videos from step 2
8. After the photos are fully uploaded, compare the auto-tagged photos to any differences in the opted-out photos/videos; this step will show us if the photos that were uploaded AFTER the opt-out option is selected, are still being recognized and marked with tags that the user can select from instead of being auto-tagged after upload.
9. Conclude from our testing if the opt-out feature is truly "OFF" when a user decides to opt-out from Facebook's facial recognition usage/auto-tagging. To discern this we will be able to infer from the tagging options whether the tags presented are the same from the tags that were presented for auto-tagg: meaning, if the tags are the same for opt-out tags and auto-tags then the software is still scanning regardless if the opt-out feature is chosen or not.

After conducting these series of events, we will be able to conclude whether or not Facebook claims to allow its users to keep the auto-tagging feature turned "OFF" or if behind the scenes they may still be scanning every photo and video through their face-matching photo-tagging software.

2. By observing the packets transmitted by Facebook from their user interface

With the understanding of what information Facebook is allowed to process and store, the next goal is to ensure Facebook is following the standards set in place by their own policies, such as their privacy policy, in regard to image data. However, before any interpretation can be made, the data must first be collected. In order to collect the traffic Facebook's web client transmits, we will be using Wireshark to capture raw packets and Postman to follow and organize HTTP/HTTPS traffic.

To capture the transmitted packets, we will use the following procedure in Wireshark:

1. Begin capturing packets in Wireshark. This will also capture large amounts of superfluous data, but this can be filtered out.
2. Login to Facebook using a new account. This account should not have any associations to previous data (such as using personal accounts) as to avoid any distortion of what information Facebook gathers.
3. Upload a photo to Facebook.

   a. Change the account's profile picture to a different photo.

   b. Post a photo to the account's feed without text.

   c. Post a photo to the account's feed with relevant text, such as a caption.
4. Stop capturing packets in Wireshark, and then gather the relevant traffic and export to a capture file. This file will later be searched for any traffic which contains data that is not explicitly permitted according to our findings from policy and legal research.

Delivery Stage

- We will compile all of our findings into our Github's project readme document and files

- We will conclude from our discoveries if the social media usage implications are made succinct in Facebook's policies

- We will create a report and presentation on our results from our testing outlined above

Resources Needed

Resource	Dr. Hale needed?	Investigating Team member	Description
Facebook policies	No	Caroline	Digging in to the policies to see how the data is used within Facebook
Facebook Open Source Library	No	Entire Team	Digging into the library to exam how the data is used and transferred in to Facebook storage. Examples: DeepFace
Library Database	No	Entire Team	Using Library Database to gather backgrpund information on facial recognitions
Lua	No	Entire Team	Programming Language of DeepFace and MultiPathNet

First Sprint Plan

GitHubs Kanban Board

Issues for Sprint 1

1. Review and test opt-out option for Facebook's facial recognition
2. Research convolutional neural networks (CNNs) and how they are significant to Facebook's AI research

Presentation Video

M1 Video