**6.170 - Fall 2015**
**Team Abu Mongoose**
Noor Eddin Amer | Suniyya Waraich | Usman Ayyaz | Angus Lai

# Occasional Thoughts - Design Document

# Overview

## Motivation

### Description of System

We will be building a system that allows a user to create a collage of posts in celebration of a specific occasion. The occasion could be a friend's birthday, a sibling's graduation party, or a baby shower - basically anything worth remembering. A user can create what we will call an *occasion* that is populated with *thoughts.* A thought can be a message to the person whose occasion is being celebrated, a message related to the occasion itself or a picture with a comment. The creator of the occasion shares the link with specific people who can add their thoughts to the occasion. The result is a collage of pictures and messages that can be shared with relevant parties to be cherished by them, forever.

### Purposes

1. To celebrate an occasion by inviting friends to share their thoughts about the occasion.
2. To allow people to add their thoughts without physically being at the occasion
3. To regulate who gets to participate in the occasion collage.

### Deficiencies of Existing Solutions:

One existing solution is a physical card (a paper card), that can be bought for an occasion, signed by different people and given to the intended person. But it is often hard to get all the needed people to sign it. Some might not be in town. Conversely, sometimes the card might end up being passed around in a large room and people who are not relevant to the occasion may end up signing it too. There is also the added problem of someone feeling uncomfortable with other people reading the message they wrote to the receiver, which they intend to be private. All of these issues are dealt with by our app. It makes things hassle-free, more efficient with the added advantage of having a copy of the messages that will most likely last longer than a piece of paper.

An existing technical solution is a Facebook event wall. A user can create an event page and share it with relevant parties. The relevant parties can in turn post to the event wall. In this context, the event wall can serve the purpose of an occasion and posts can serve the purpose of thoughts. However, Facebook events are not used in this way because they have some key deficiencies. First, the primary purpose of a Facebook event page is not to produce an event collage, but rather to provide the event description and show who is attending it. Under this user model, users use the event's wall for inquiries and announcements rather than to produce an occasion collage. Secondly, if we assume that users will want to use the Facebook event wall to produce a memoir of the occasion, then all posts would be public to viewers. However, our app addresses this issue

by enabling users to specify whether their thought should be viewable by any participant or just the recipient.

# Design Essence

## Concepts

### Occasion

*Definition:* A way to consolidate and share occasion-specific thoughts.

*Purpose*: to provide one place where people's memories and wishes can be consolidate easily in celebration of an occasion.

*Operational Principle*: A user can create an occasion and share the link to the occasion with other people, with which users can view and add content to the occasion.

### Thought

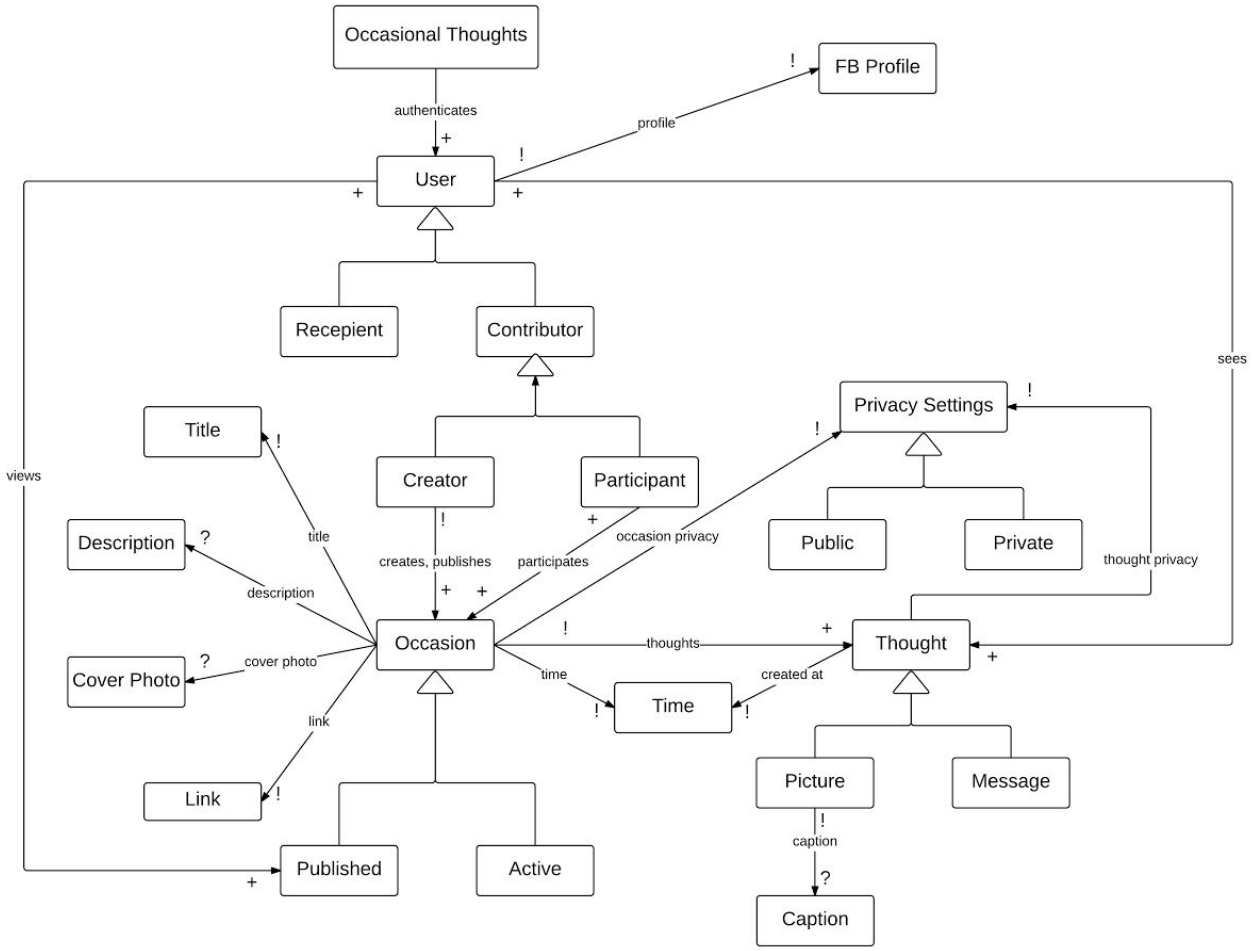
*Definition:* A picture, a wish or a message published on an occasion, the smallest unit of content that can be added to an occasion.

*Purpose*: to contribute a message or picture to an occasion.

*Operational Principle*: If a user is invited to contribute to an occasion, they can share their thoughts on the occasion page.

# Data model

## Diagram




## Explanation

Occasional Thoughts authenticates users using facebook login. Afterwards, a user can create an occasion (making him the creator) and share it (using facebook in our final version) with other people. These people (participants in this case) on visiting the page will be similarly logged in and then will be able to add thoughts and contribute to the occasion.

Privacy Settings: A thought and an occasion can either be private or public. As explained in the textual constraints, private thoughts and occasions are only viewable by recipients and the creator. Public thoughts are viewable by recipients, participants, and the creator.

## Textual Constraints

1. The creator can always view all thoughts and occasions.
2. If a thought's (or an occasion's) privacy is set to private, then users who are recipients can also view it.
3. If a thought's (or an occasion's) privacy is set to public, then all users can view it (recipients, participants and the creator).
4. Authentication occurs using the facebook API (so if a user is not a facebook user they won't be able to proceed).
5. A message must be a non-empty string with no media attached.
6. A video cannot be uploaded in place of the picture.

## Insights

We created the contributor set to indicate that both the occasion creator and participants can contribute to it.

We used facebook authentication in part so we could fetch a user's profile picture along with their name. This is so that if two participants who have the same first name, write messages in the occasion (no pictures), they may be distinguishable by their profile pictures (which we can have appear next to their thought and name in the UI). Additionally, fetching data from facebook will allow us to have access to their extended user base, which gives a better user experience when it comes to sharing the link of an occasion.

The creator can publish an occasion which will close the occasion so that no one can share thoughts on it later. The occasion page will stop being an editable link and become a kind of a collage. The collage (set of thoughts) will look different for each user depending on the privacy settings of the thoughts. The participants may not be able to access the occasion once it's published depending on the privacy settings the creator chooses.

We had the idea to incorporate the above publish functionality, in order to solve a usability problem: Suppose a user creates an occasion and shares the occasion with other friends. When any of these friends will open the occasion, they will see a page full of already posted thoughts (depending on which they are permitted to view), in addition to a textbox reading "Add a thought!", in which they can submit their thoughts. But once the page is ready and we share it with the intended recipient, we don't want the textbox to show. So we transform the page to get rid of the textbox.

*Comment:*
In our model, the situation in which two people create an occasion for the same recipient, with the same title and purpose in mind is not affected. Our model allows any number of users to create an occasion with the same name (and same purpose in mind). This is not a problem because each occasion will be linked to its creator so there won't really be any confusion.

# Security concerns

## Key Security Requirements

*Authentication*: All content require authentication. To implement this, we require that all users be authenticated with Facebook login.

*Content control*: The person who adds the content can control the privacy settings of the content, ie., the person who creates an occasion defines a list of users (participants) who can add a thought or make it public through a link. He also defines a list of intended users who can view all thoughts of that occasion (recipients). The person who adds a thought can choose whether that thought is visible to only the intended viewers (ie. creator and recipients) or visible also to anyone who has the permission to add a thought (ie. visible to creator, participants, and recipients).

*Dealing with links:* Since the use of links is key to this product, the main security threat is in preventing unintended people from accessing those links. We will protect our user data by using a hash for each link instead of the event name. We will use the occasion's object id generated by mongo instead of the occasion's title. This will prevent unintended people from gaining any information about the occasion. To guarantee that only intended users can access the links, we will require facebook authentication to access the links (whether you're the creator, a participant or a recipient). Upon landing the site, the user will be asked to login, and if the occasion's privacy settings disallows the given user from accessing the occasion, then we return a 404, meaning they won't gain any information about occasion hashes, in addition to not being able to view or contribute to the occasion.

## Mitigating Standard Web Attacks

*XSS Code injection*: As a rule, we do not trust any content provided from the client side. Therefore, the responsibility for sanitizing all inputs lies with the server. To handle code injection, we will sanitize the inputs through the use of existing libraries.

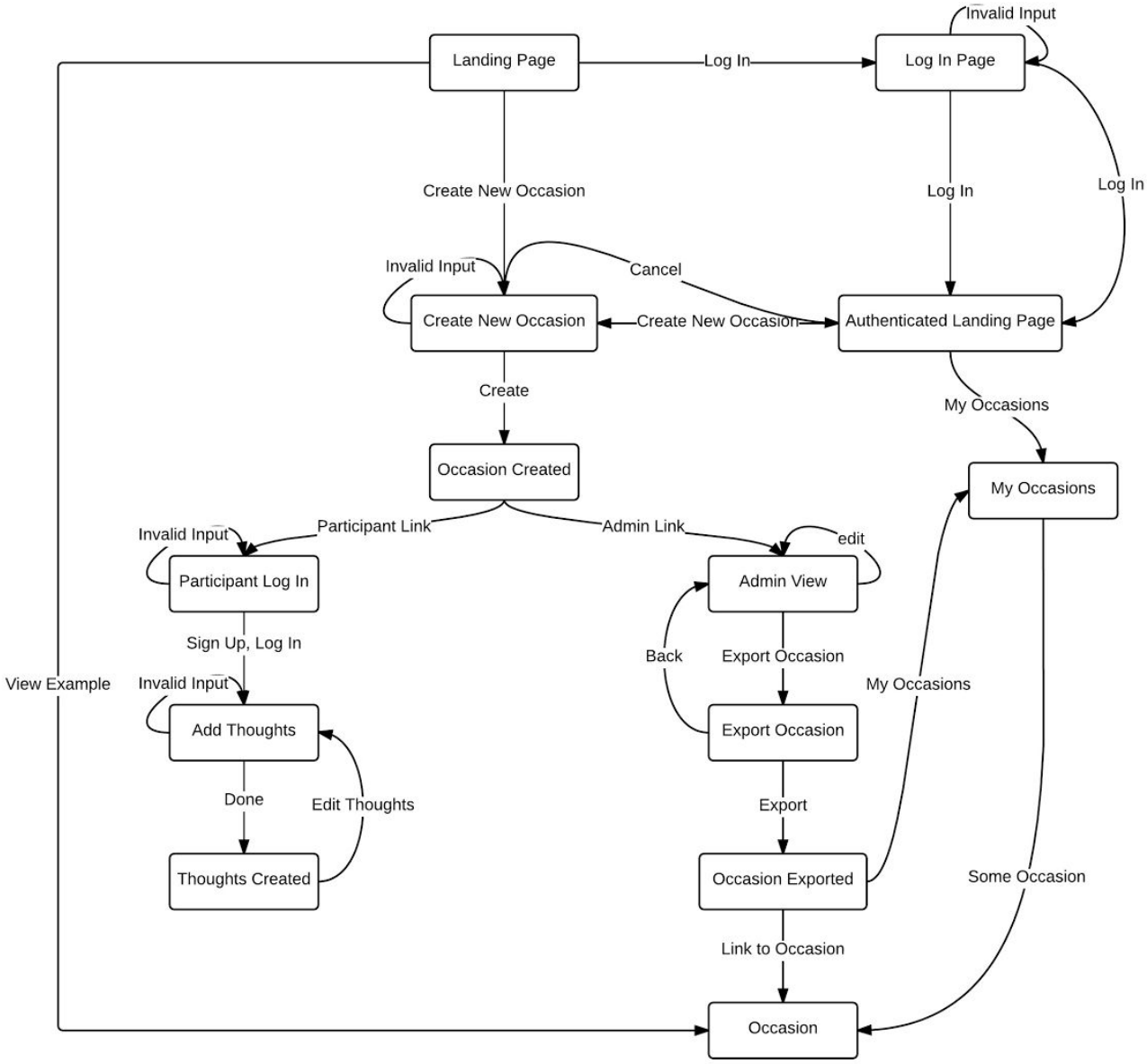
*Cross Site Request Forgery*: We use session tokens and TSL to defend against CSRF. Whenever we send a form that asks for a user input, we send along a session-specific token, which the user then sends back when they submit the form. To prevent man-in-the-middle attacks, we use TSL. This verifies the authenticity of the content.

## Threat Model

- We assume that the attacker can send any requests to the servers.
- We assume that attackers do not have access to our servers.
- We assume that users can be attackers.
- We assume that a benign user can be controlled by an attacker.

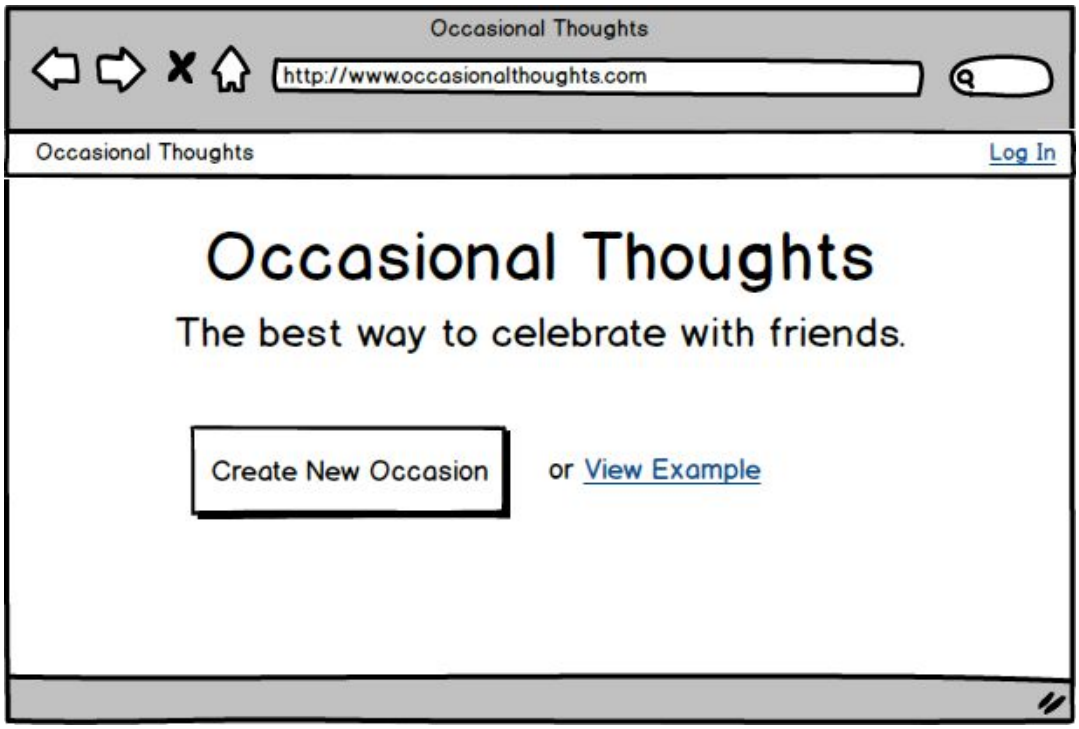
# User Interface

## Transition Diagram

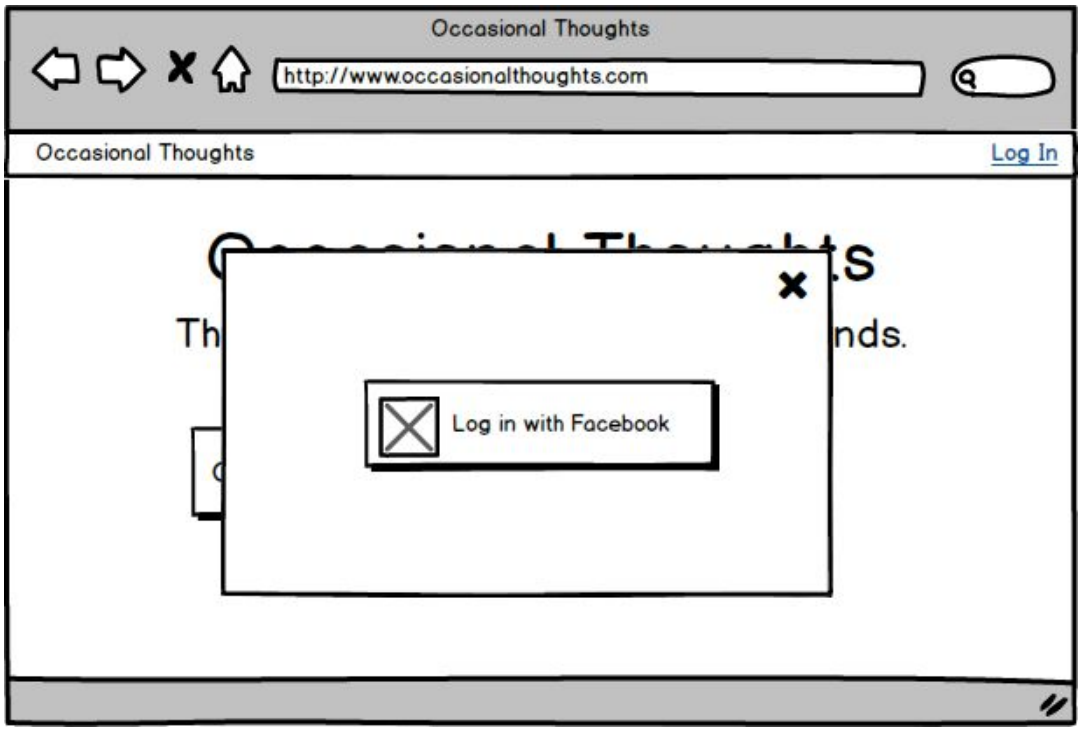


## Wire Frames

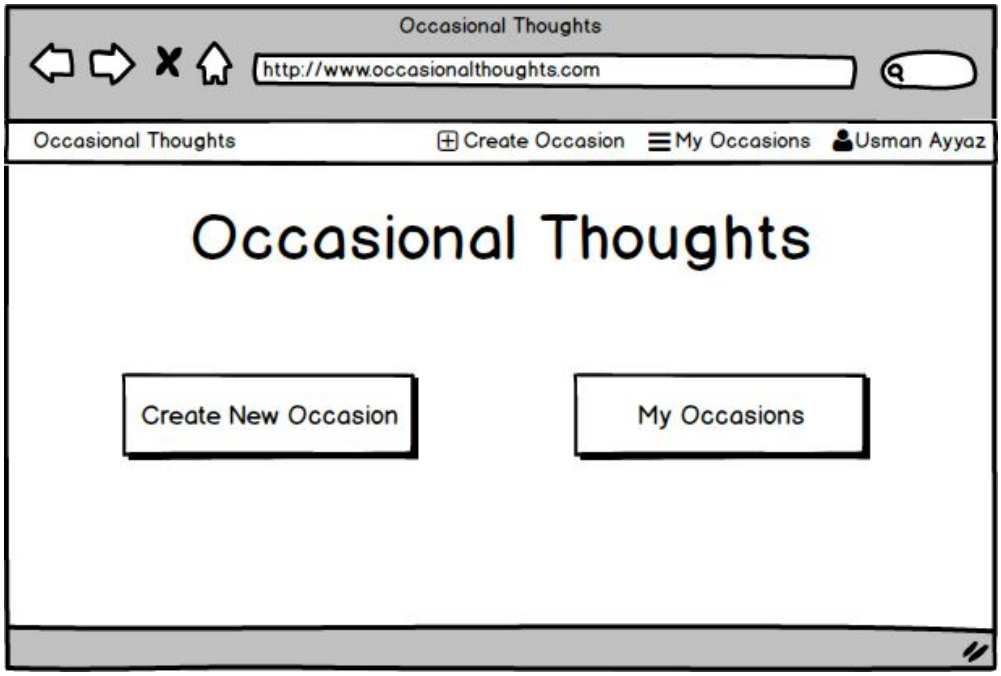
*Landing Page:*



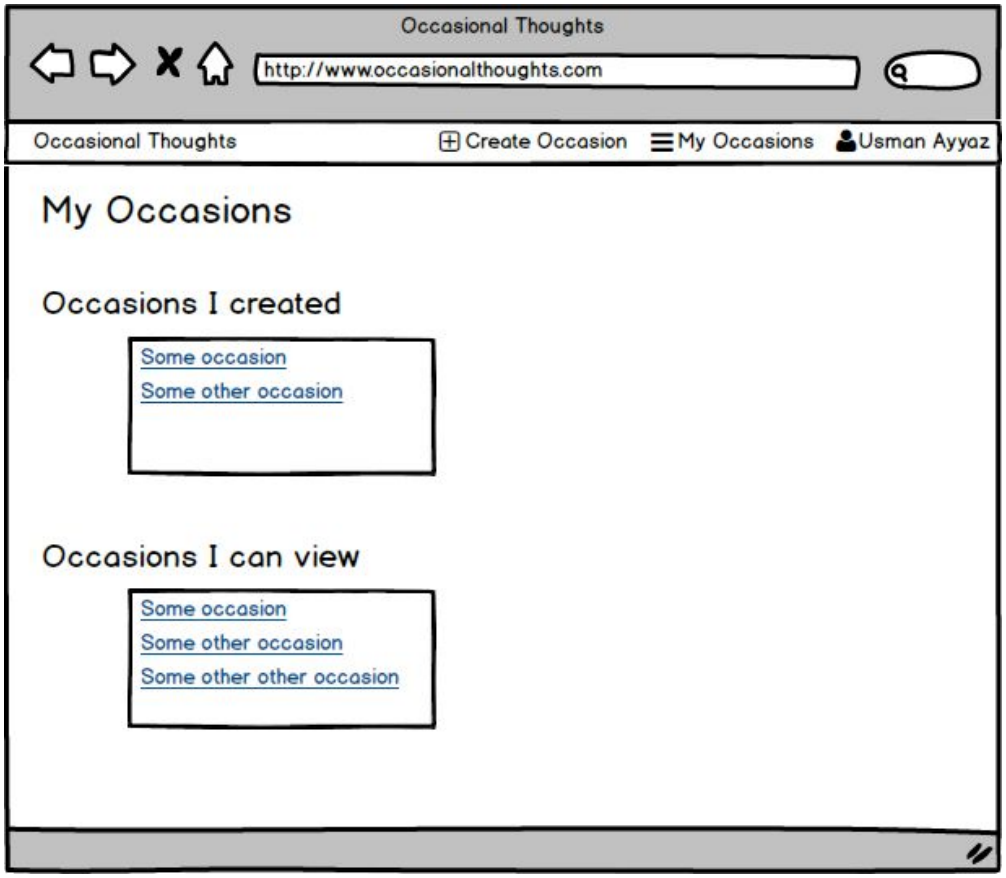

*Log In Page:*



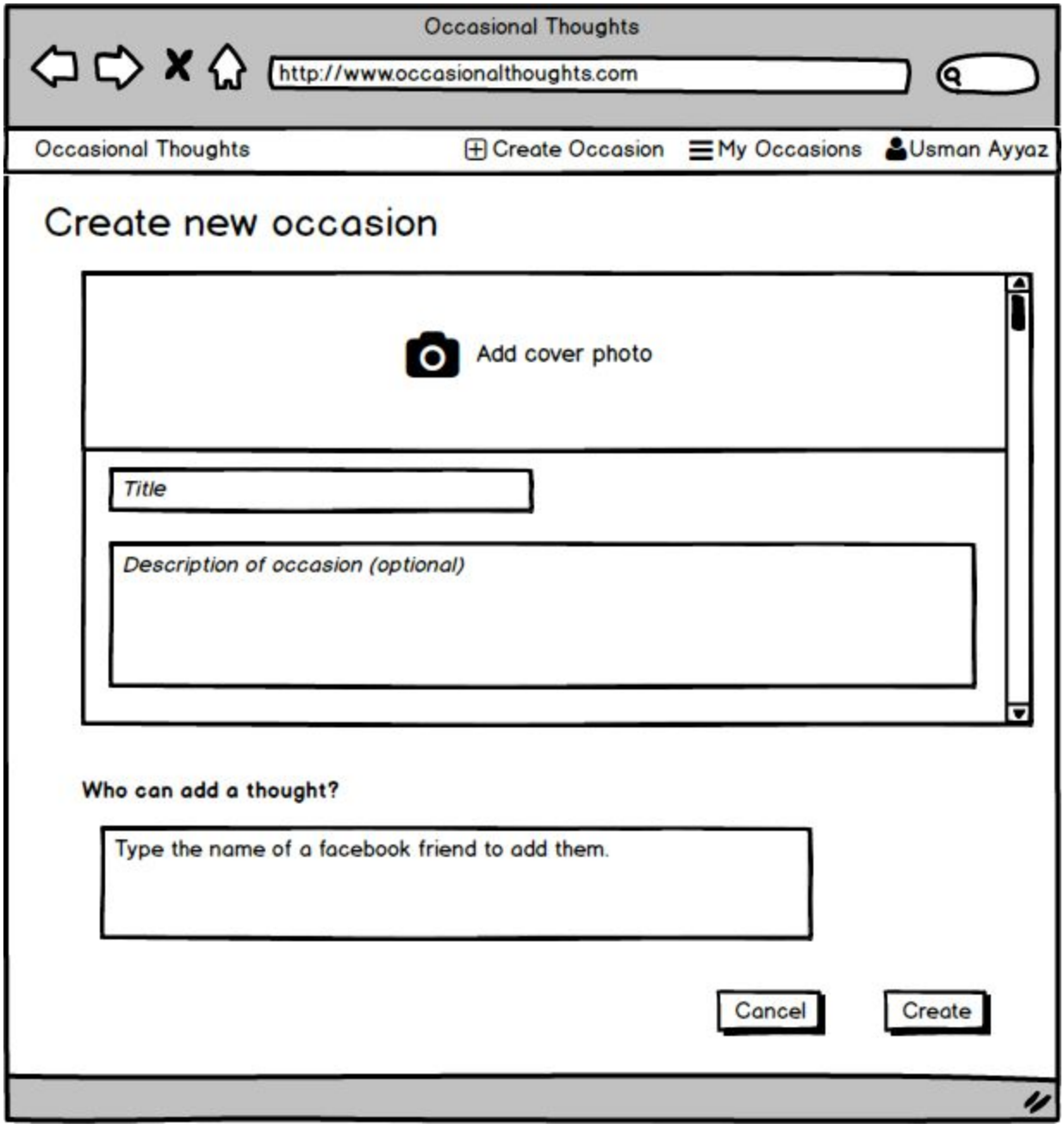
*Authenticated Landing Page:*




*My Occasions:*

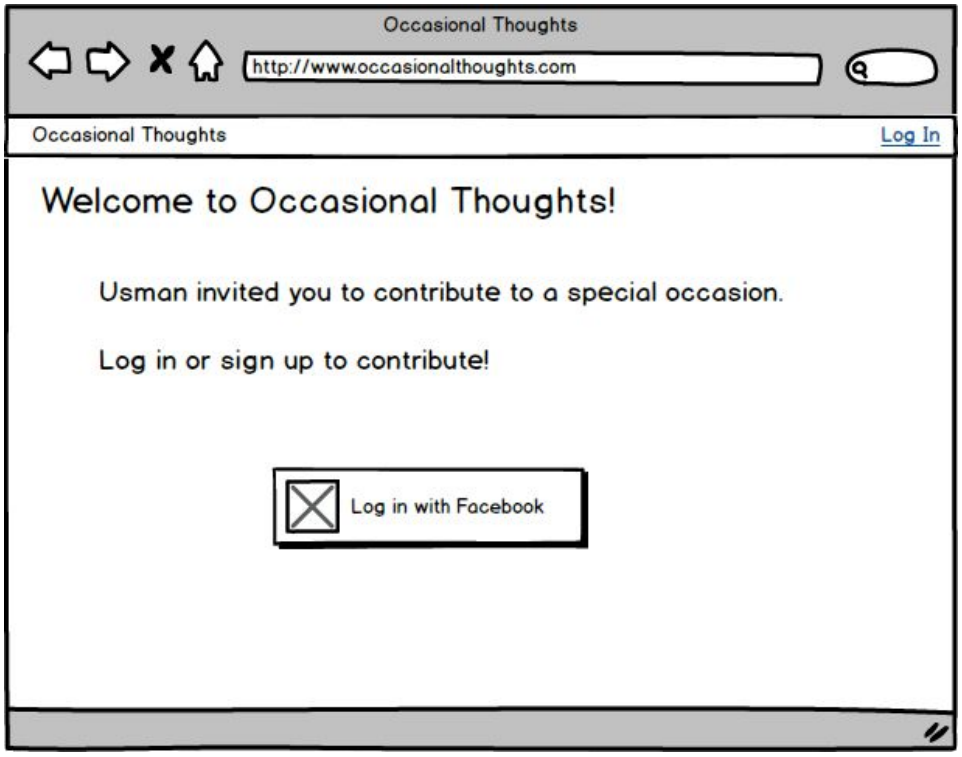


*Create New Occasion:*

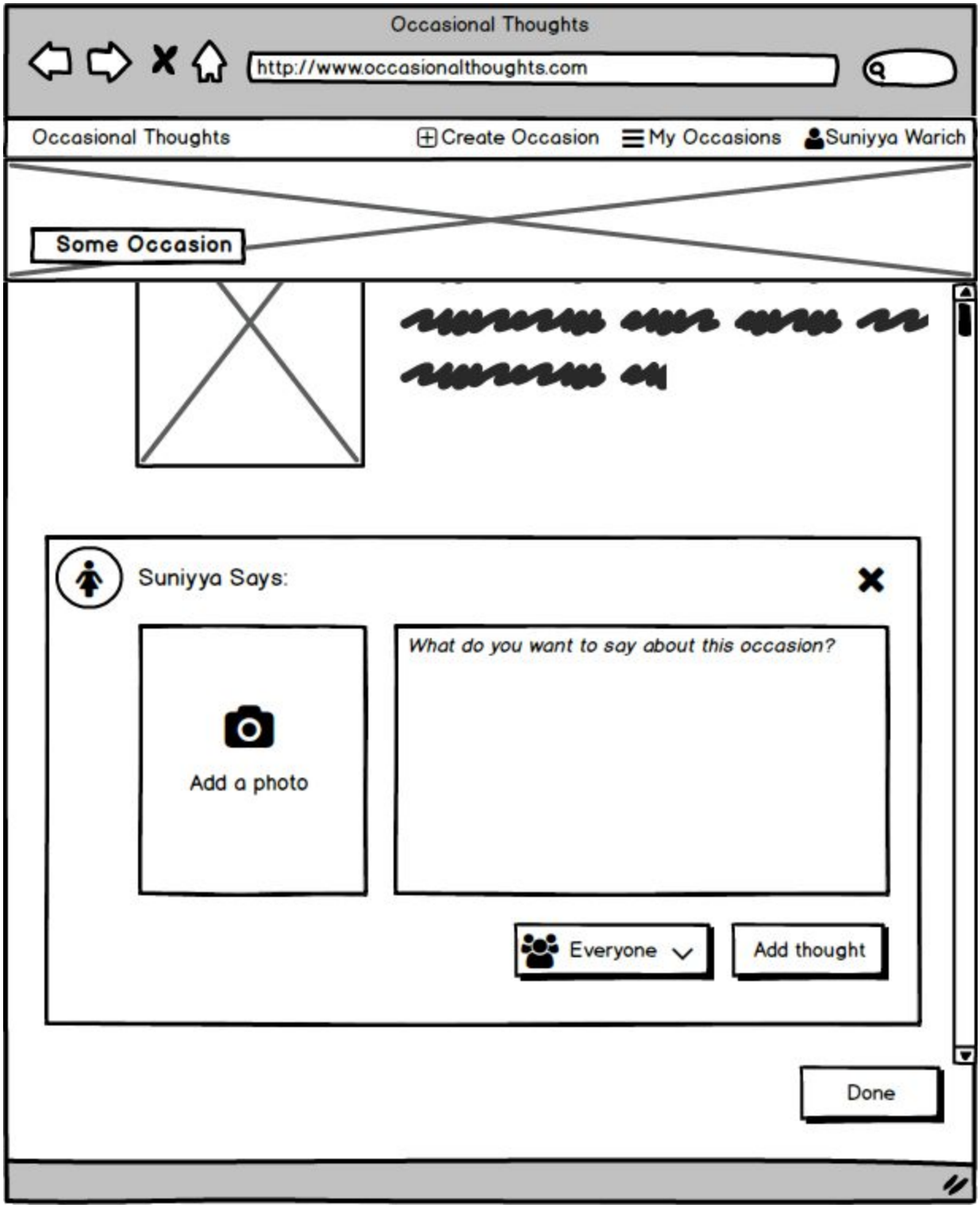


*Occasion Created:*

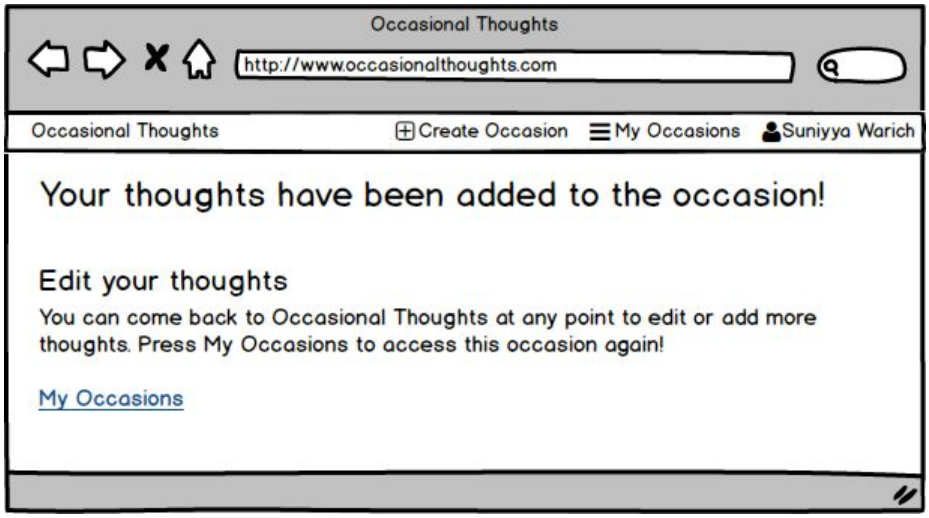

*Participant Log In:*



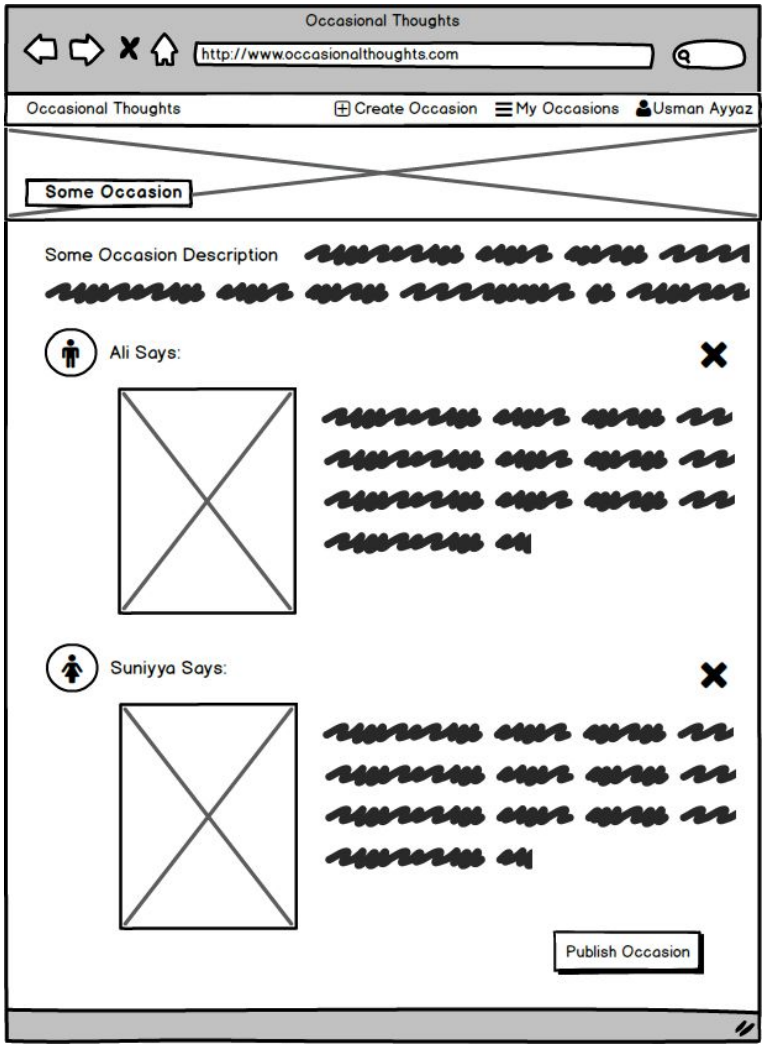
*Add Thoughts:*



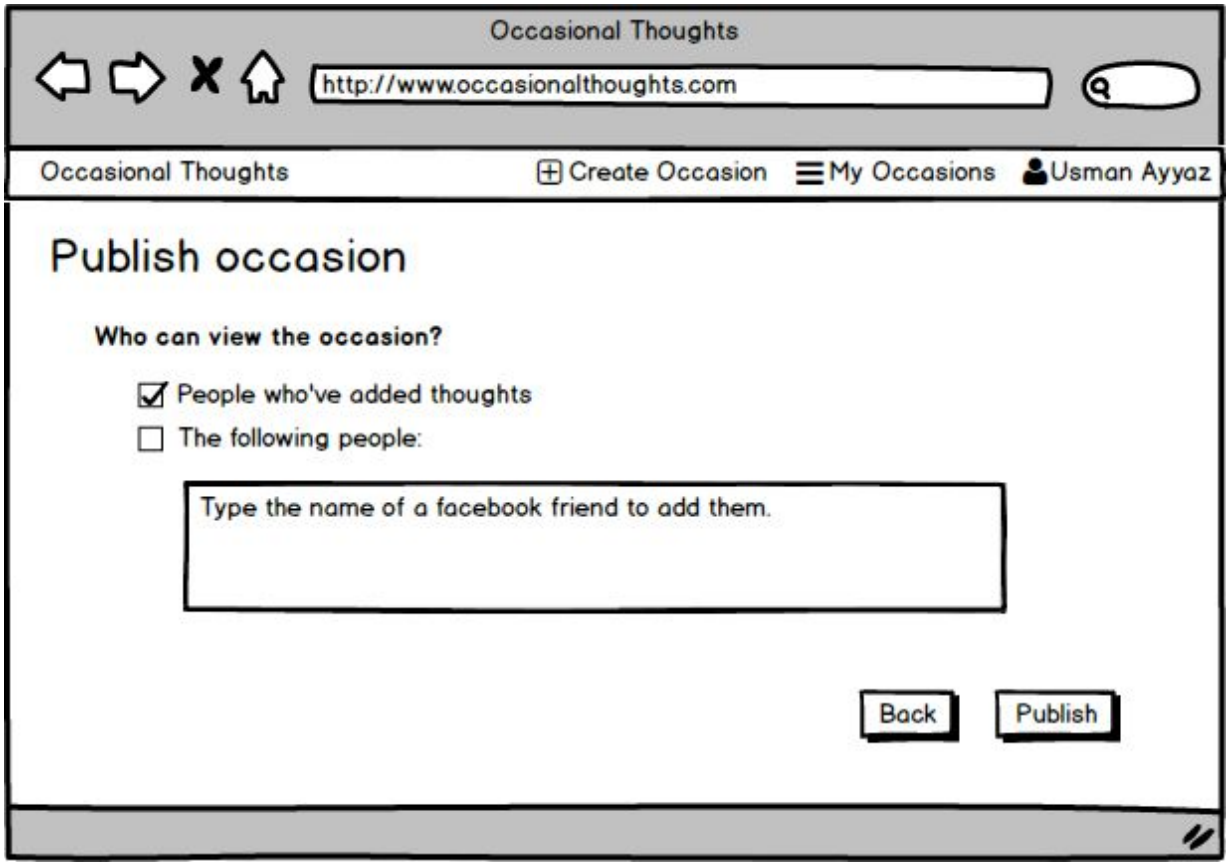
*Thoughts Created:*



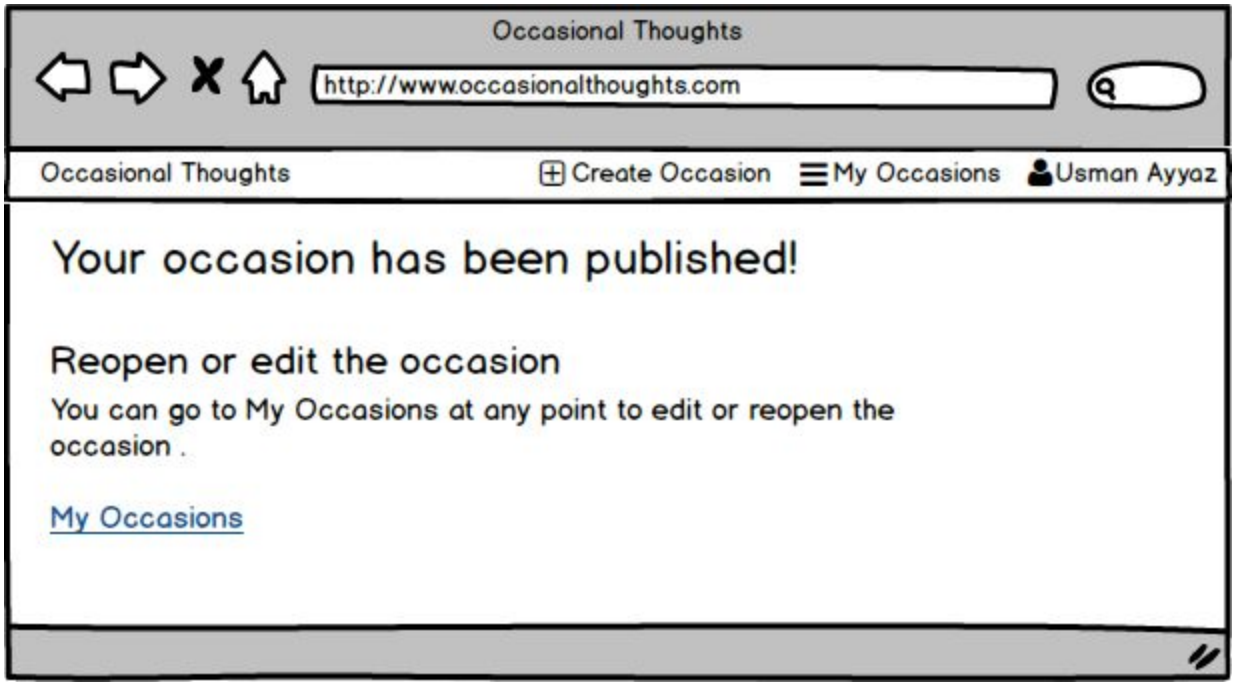

*Admin View:*



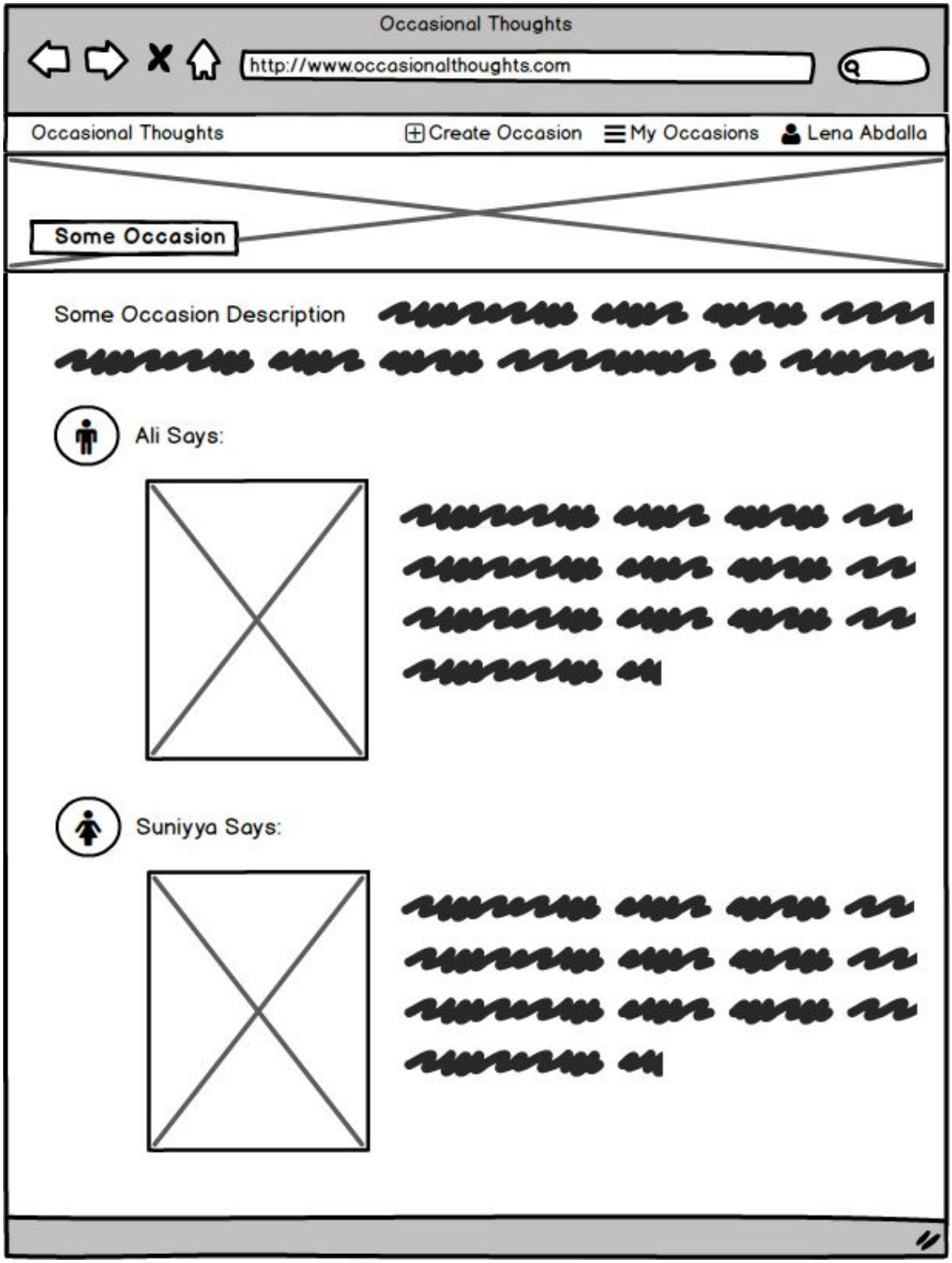
*Export Occasion:*




*Occasion Exported:*



*Occasion:*


Occasional Thoughts
http://www.occasionalthoughts.com
Occasional Thoughts
Create Occasion
My Occasions
Lena Abdalla
Some Occasion
Some Occasion Description
Ali Says:
Suniyya Says:

# Challenges

## Design challenges

### User Authentication

*Problem*: Since this app is largely link based, the idea of a user account may not be present in the user model of occasional thoughts. In other words, users don't expect to have a profile like they would in facebook or twitter.

*Potential Solution:*

- *Use no authentication.*
  Under this approach anyone can come in and create a link. They then have the responsibility of sharing that link with people they want to add thoughts. That user can then export the occasion and share it with intended recipients (we have a few options here: we can either use the computer's IP address to figure out who created the occasion, we can only require the occasion creator to log in, or we can give everyone the ability to publish the occasion and the responsibility of publishing and sharing the occasion collage will be in the hands of the people creating it). This approach has the advantage of requiring no user authentication at all. It's obvious drawback is the absolute lack of privacy and the vulnerability to attacks.
- *Rely on a conventional user registration and login with an email and a password.*
  This way any person can login. Additionally, we can use the user's provided emails to make the sharing of occasions easier (ex. autocomplete when listing emails to share the occasion with etc …). There are a few cons to this approach, however. First, the user will have to remember a password and since this application is largely link based they may not have the tolerance to remember the password of one more application that they do not frequently user. Additionally, to get a user profile photo, the user must upload a picture directly. Similarly, any further information we require from the user must be provided directly by them.
- *Use facebook authentication.*
  This approach is a lot similar since the user does not have to manually enter any information. Logging in is a button away. We can access the user's profile picture, email address and name directly from facebook. An additional advantage is that we can access the user's list of facebook friends and use that list when sharing the occasion with friends. A drawback of this approach is that non-facebook users will not be able to use the application.
- *Use facebook authentication with the added ability of registering with an email.*
  This option incorporates the previous two options. It therefore, inherits the advantages of both approaches. However, this approach will be technically more demanding.

Additionally, sharing will be complicated. If sharing occasions is going to be through facebook friends, then people who signed up through email won't be able to use that feature.

*Chosen Solution: User facebook authentication.*
We chose to use only facebook authentication. This seemed like the best option given the scope of this project. In retrospect, the targeted users for this app will most likely have facebook accounts. Additionally, forcing the idea of having a facebook account will make the user experience a lot smoother.

## Unwanted Thoughts

*Problem*: Some participants may add thoughts that are unwanted. The viewers of the occasion may not want to see thoughts containing vulgar, insensitive or negative thoughts.

*Potential Solution:* To solve this problem we have made the following design choices:

- *Keep all thoughts as is.*
  Under this approach, you trust the participants to be considerate in entering their thoughts. In the off chance that someone provides an unwanted thought, then that unwanted thought will simply be part of the occasion collage. This approach has the obvious drawback of providing no mechanism of countering unwanted thoughts if they prove to be a real issue.
- *Make the creator the moderator of all content.*
  The creator of the event will act as a moderator of the content of the occasion. Before exporting the occasion she will have the option of removing any unwanted thoughts. One caveat is that if another participant views the page before the creator edits it and they have permission to view the content of unwanted thoughts, they will see that content.
- *Require the creator's approval before adding thoughts to the occasion.*
  This approach will guarantee that no unwanted thoughts will make their way to the occasion collage. However, this approach requires an unreasonable amount of the creator's time and attention.

*Chosen Solution: Make the creator the moderator of all content.*
This approach provides a mechanism for monitoring the content of the occasion while still allowing the process to be straightforward and not too much time intensive.

## Privacy Concerns

*Problem*: The content that the participants produce may be embarrassing, personal or sensitive. In all of these cases, participants may want such content to only be visible to certain users and not others.

*Potential Solutions:*

- *Make all thoughts public by default.*
  This is not a solution to the problem, but it rests on the assumption that this issue will not come up. Specifically, this approach forces users to avoid adding thoughts that are embarrassing, personal or sensitive. This will surely take back from the user experience, as such thoughts are usually the most valuable to the recipients.
- *Each user can choose specific people who can view their thought.*
  This is the ideal solution, but it is too intensive on the user's side. Additionally, users may not know exactly who they want to view the thought. They may want for instance to only prevent certain people from seeing it, instead of picking who to see it.
- *The creator can view all thoughts and the user can choose between only allowing the recipients to view their thought or allowing everyone to do so.*
  This solution gives the person adding the thought one of two choices, either have everyone see your thought or only the recipients of the collage see it. This is a fair proposition, particularly since all thoughts should be addressed to the recipients. This approach also places an implicit trust in the creator as the moderator of the whole process.

*Chosen Solution: The creator can view all thoughts and the user can choose between only allowing the recipients to view their thought or allowing everyone to do so.*
The creator of the event can see all the thoughts added by participants. This fits with the user model since they are clearly invited by the creator to add a thought. This also has the added advantage of using the creator as a moderator and a filter of any unwanted thoughts. The creator also controls who can access the occasion. This will solve the problem of who can access the occasion. Participants can further choose who will be able to view the thoughts they added. That way participants will feel comfortable sharing personal thoughts.

## Occasion Sharing

*Problem*: How should the occasion sharing process work? Which user experience would best accomplish this purpose? Since there may be some privacy issues with who can view or contribute to an occasion, this problem becomes more complicated.

*Potential Solutions:*
- *Generate a link to the occasion and leave the sharing to the creator.*
  This approach is the simplest. The app will generate a link that the creator can then share with the intended contributors and viewers (through email, facebook etc…). While this approach is the simplest, it has serious security implications. Anyone with the link can access the occasion.
- *Have the creator type the emails of people to share the link with.*
  This solution guarantees security, however, it is work intensive on the creator. No one remembers a handful of emails by heart!

- *Have the creator choose the people to share the link with from their list of friends.*
  This approach solves the privacy issue while not requiring the creator remember email addresses. All they need to do is remember the names of people they want to invite. A disadvantage here, is that the creator won't be able to invite non-facebook friends to contribute to the occasion.
- *Create a notion of friends within the app and have the user choose from them.*
  This solution is the most technically demanding. The number of users of the app will also be much lower than facebook users, hence hindering the usability of the product as a whole.

*Chosen Solution: Have the creator choose the people to share the link with from their list of friends.*
This seems to be like the best solution to the proposed problem. It allows for a simple user experience while addressing security concerns.