Should I ShareThis?

Support awareness of social media sharing practice that might compromise online privacy and reputation

Jaewon Hwang

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Design

University of Washington
2016

Committee:
Jason O. Germany, Chair
Dominic Muren
Sang-gyeun Ahn

Program Authorized to Offer Degree:
Art

University of Washington

Abstract

Should I Share This?
Jaewon Hwang

Chair of the Supervisory Committee:
Jason O. Germany, Assistant Professor
Industrial Design

People on social media share information about themselves or others to maintain and expand their relationships. In doing so, they can put at risk their privacy and the privacy of people they know. The intentional or unintentional posting of inappropriate content online can lead to serious social, professional and even legal ramifications, depending on the nature and severity of the shared content.

This project investigates how various social media products implement user interfaces that help users manage their privacy preferences and the gap between the way they actually manage their privacy and reputation organically in the course of using said products. Additionally, this project demonstrates how design can help support awareness of social media sharing practices that might compromise online privacy and reputation. This resulting design and research insights from this project aim to shape a new model of these virtual and social interactions.

Table of Content

Why Privacy Matters

As information becomes increasingly more open and accessible, it is becoming evermore challenging to keep our private information private. However, safeguarding individual privacy is very often not a priority when new products are designed, and current implementations are mostly after thoughts and can be cumbersome to use. In many ways, internet service companies that help people share their ideas, thoughts, feelings and captured moments of their lives are incentivized to encourage liberal sharing, even at the expense of individual privacy.

According to an article by Anne Gammon 'Social media blunders cause more damage to important relationships today than two years ago' on YouGov Omnibus blog, 57 percent of US adults who use social media have published content that they later regret sharing.[1] One in six regret a post at least once a week (these numbers vary depending on age). Also this survey reveals an interesting change in their privacy concern. Among participants, 21 percent of them are worried they might negatively affect their careers with a questionable content. Also, the survey reveals their biggest social media regrets as 36 percent regretted that they didn't properly consider a response and they sounded foolish. 29 percent made a comment in the heat of the moment and offended some people. Taken as a whole, 57 percent of social media users have posted something that they regret afterwards.

Designing with user privacy as a first priority can help people be more aware of their privacy and reputation online. Social media filter, as a concept platform, proposes one way for social media companies to put privacy first when they design a new product.

1. Anne Gammon. "Social Media Blunders Cause More Damage to Important Relationships Today than Two Years Ago." YouGov. July 22, 2015, https://today.yougov.com/news/2015/07/22/social-media-blunders-cause-more-damage-important-/.

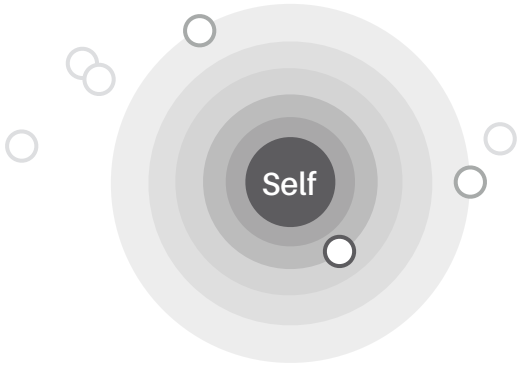


Figure 1
The variable degree of openness

Understanding Privacy

According to social psychologist Irwin Altman, privacy can be defined as the variable degree of openness one has about oneself to others (Figure 1).[2] Managing this openness is a dynamic process (Figure 2), where the final goal is to equate the actual degree of one's openness to the desired level of exposure (Figure 3). If the actual degree of privacy is greater than the desired level, people will feel isolated (Figure 4). On the other hand, if the actual degree of privacy is smaller than the desired one, they feel over exposed (Figure 5). This theory was developed in 1975, long before the rise of social media, therefore Altman's theory explains individuals' privacy in the physical world. However, I found this theory relevant to online privacy and it helped me significantly in shaping what privacy means online and how to approach this problem.

Building off from Altman's theory, privacy in this project is not synonymous with anonymity. Privacy is contextual and dynamic, rather than absolute and static. Privacy is a shifting level of exposure one seeks out regarding the exposure of one's private information to others. This level of exposure varies every time someone shares information online depending on the context. It is about how many social interactions one has and with how many they seek out online. Sometimes people want to share information with a large number of people, and other time, they want to share information with a few close people. In the former case, even if the actual level does not match with the level they pursue, it is not a privacy issue, even if they may feel isolated or lonely in the digital world. However, in the latter case, if the information is exposed to more people than they intended, it becomes a privacy issue because they feel overly exposed. This project focuses on the unwanted exposure of personal information online.

2. Irwin Altman. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Brooks/Cole Publishing Company, Monterey, California, 1975.

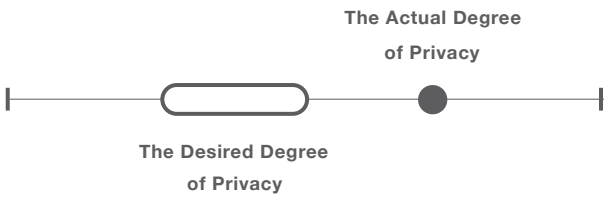


Figure 2
The two different levels of privacy

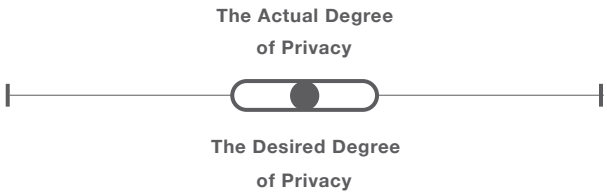


Figure 3
The goal of managing the openness

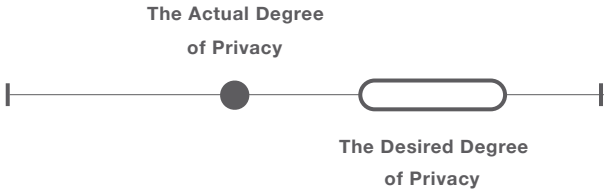


Figure 4
The levels when people feel isolated

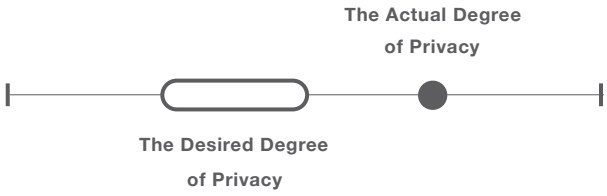


Figure 5
The levels when people feel crowded or exposed

Intended Purposes
"It's cool", "It's funny", venting frustration, good intentions, "I didn't think about it", and "Hot" states

Posted Content
Alcohol & illegal drug use, religion & politics, profanity & obscenity, sex, personal & family issues, and work & company

Unintended Audience & Underestimated Consequences
Coworkers, clients, friends, and strangers

Regrets
Embarrassment, argument, job loss, arrest, and lawsuit

Figure 6
The flow from posts to regrets

Why People Post and Regret

A flight student from Egypt had to leave the U.S. by July for posting an emotionally charged political opinion about a politician on Facebook.[3] What the student posted was perceived as a threat to the politician. Some people may think it is common sense not to post something like this in the first place. However, anyone's mistakes on social media could backfire anytime in negative ways. When people post something online, they expect their content to be perceived in the way they intended, but according to Nissenbaum, different norms and contexts coexist on social media and they can conflict.[4] It points out that one's context may conflict with others' social norms of context.

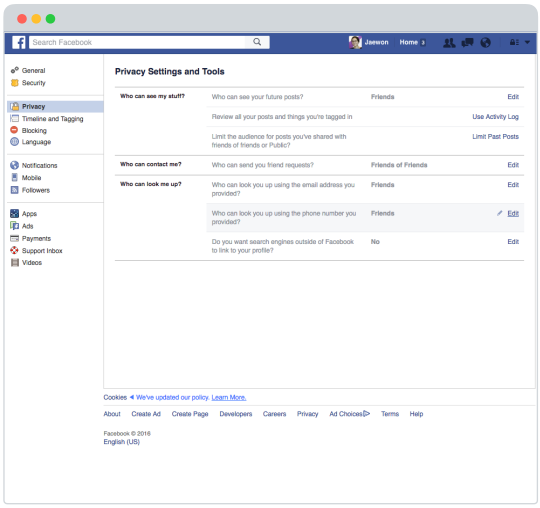
Why do people make mistakes? According to a study 'I regretted the minute I pressed share' by researchers at Carnegie Mellon University, people feel regret on social media because they make the following mistakes: unintended audience, underestimated consequences, and usability of Settings or social media platform (Figure 6).[5] There are many studies and designs that look to improve the usability issues, but this project shifts the focus towards the first two causes: unintended audiences and underestimated consequences.

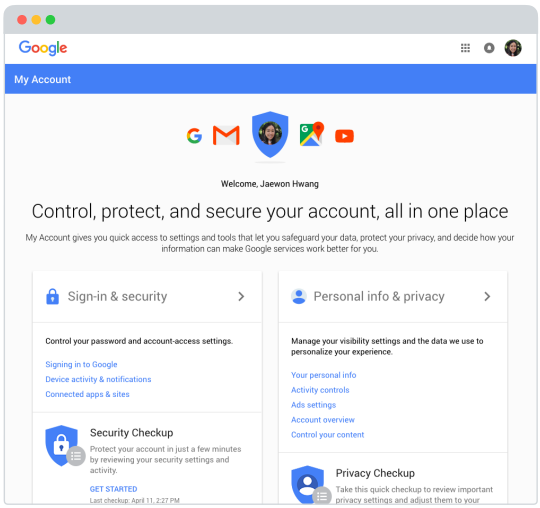
Building on top of this study, when people's posts are not perceived in the way they expected and produce negative responses, they review the responses, edit or delete the content, or 'unfriend' someone. So the management process can be divided into four steps: Idea, post, review and take action. In this process, I realized that the privacy decisions need to be made before the content gets published and managing privacy is not well supported through existing "settings" UI.

3. Liam Stack. "Egyptian Aviation Student Who Made Trump Threat Is Leaving U.S." The New York Times. March 7, 2016, http://www.nytimes.
4. Helen Nissenbaum. "Privacy as Contextual Integrity." Forthcoming: Washington Law Review, 2004.
5. Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. ""I Regretted the Minute I Pressed Share"" Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11, 2011.

Thesis Documentation

People are asked manage their privacy through Settings.





Managing Privacy 1: Within the Settings

In the physical world, people organically manage their privacy by instinct in the very moment of decisions. On the other hand, they are asked to manage their privacy through Settings in the digital world. So many Internet companies like Facebook and Google try to solve these issues by giving users a great deal of control over the collection and distribution of their personal information by allowing them to adjust various preferences. Based on an analysis of the preference settings found in various social platforms (Facebook, Google, etc) (Figure 7 and 8), I have outlined the leading challenges exhibited in these UI approaches:

Figure 7
The Settings on Facebook
Figure 8
The Settings on Google

Thesis Documentation

The Settings can be cumbersome to use.

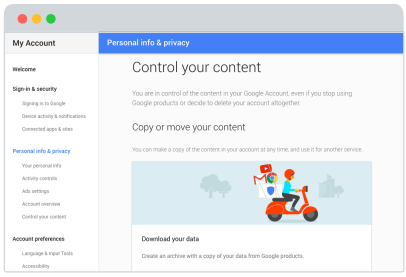


Figure 9
The Privacy Settings on Google

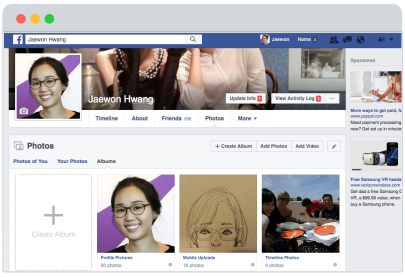


Figure 10
The Album page on Facebook

Motivation

People lack the motivation to expend the effort required to study various privacy settings. The benefits of investing the time is not immediate nor apparent. (Figure 9)

Conflicting Preferences

Some combination of preferences can result in ambiguity. For example, when a user tags a person on a private photo, it is unclear whether it gets shared or remains private. (Figure 10)

Friends cannot safeguard the information users share.

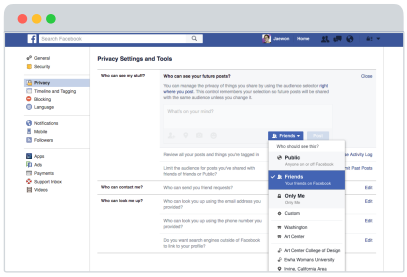


Figure 11
The audience selector under the Privacy Settings on Facebook

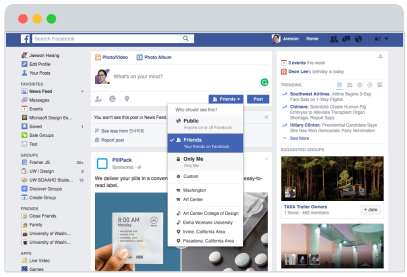


Figure 12
The in–line audience selector on Facebook

Audience Selector

Audience selector is one of most important privacy decisions to be made and there are two audience selectors on Facebook. (Figure 11 and 12). Many social media sites limit the visibility of information to friends or connections only. However, many researches indicate that younger users feel more comfortable managing privacy settings, but interestingly tend to make privacy mistakes and regret more frequently. It is because the friends or connections cannot safeguard the information users share, because many people accept friend requests from strangers. So the list of friends or connections often include people from a variety range of intimacy like actual friends, family, coworker, people they met but close, and strangers. In order to better manage privacy, people need to be more selective about the audience depending on the context of the content they are about to share.

The Settings cannot anticipate for the moment.

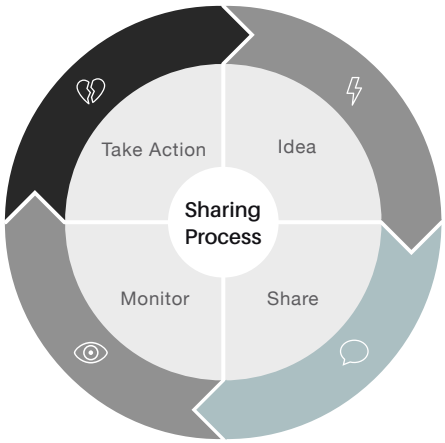


Figure 13
The sharing process on social media

The Premeditative Approach of the Settings

After researching the preferences, I realized the bigger problem of the Settings UI. It transports people away from their context to another page and require them to plan and adjust preferences well before they get an idea of what they want to share and the moment of sharing. (Figure 13) However, privacy decisions need to be made after they get an idea before they share the idea. Therefore, the approach cannot anticipate for the moment of decision and makes the decisions reactive, even though the approach is good for the general preferences of the entire platform.

Privacy Settings on Facebook

Privacy Settings is one of 14 different Settings, like Genera, Security, Language, and Notifications. Under the Privacy Settings, there are three different menus: 'Who can see my stuff?', 'Who can contact me?', and 'Who can look me up?'. The second and the third are the options for visibility of a user's profile, and the first one is the options to manage content that has been shared and select audience for the future posts.

Under the 'Who can see my stuff?' menu, there are three preferences: 'Who can see my future post?', 'Review all your posts and things you're tagged in', and "Limit the audience for posts you've shared with friends of friends or Public?'. The second is a preference to review all of the digital footprints the user has been left, including posts, comments, tags, and events, it is not the scope of this project.

The first one is a preference to select audience for the future posts and status updates. It allows users control who gets to their timeline content. Facebook encourages the users to change it to Friends, even though the default is set to Public. However, once a user selects a group of audience, the selection is applied all the content the user shares regardless of the context of the shared content. So Facebook added this audience selector into where users compose a post alongside the 'Post' button to enable the users to select different audience for different content. However, it is the same preference with the 'Who can see my future posts?', so the way it organizes the audience is still mainly three: Public, Friends, and Only Me.

Tasks that can be done through the Privacy Settings:

- Selecting a big group of audience for the future posts
- Limiting the audience for the old posts to Friends

Managing Privacy 2: Beyond the settings

According to a survey by Harris Interactive in September 2012, 75 percent of participated online U.S. adults have searched their own name and 48 percent of them found personal content they do not want to share.[6] In addition, several people I interviewed mentioned that they have another accounts to make sure that their personal content is not shared with strangers or the public and I realized that there are many other tasks people do beyond the Settings to manage their privacy and reputation. (Figure 15) Here is a list of tasks that they do to in order to manage their privacy and reputation:

- Create an fake account
- Self assessment of old posts
- Based on the assessment, delete or edit old posts
- Do not share
- Unfriend or unfollow someone
- Decline requests
- Use Privacy Settings

There is a gap between managing 'privacy settings' and managing 'privacy'.

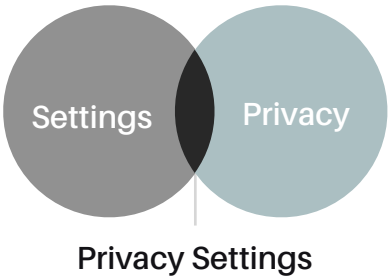


Figure 14
A gap between managing 'Privacy Settings" and managing 'Privacy'

6. "Just Google Me." Harris Interactive. September, 2012, http://blog.brandyourself.com/wp-content/uploads/Harris-FULL-Study-Report-3.pdf

Contextual, Selective, Beyond the Settings, and Preemptive

Designing with User Privacy

Facebook is the largest social media platform by far, and it is a service that evokes concerns about user privacy. However, there is no doubt that it is a leading social media service when it comes to designing for privacy in the industry. As a Product Designer in the privacy team at Facebook, Charlie Deets shared his insights on Medium (an online publishing platform) about his firsthand experience.[7] Below, he describes how he evaluates a successful privacy feature:

"I view it as a design failure if we have to send someone to a settings page. That is putting the responsibility on the person using the service to fix the problem. The settings should be coming to you when you need them."
– Charlie Deets, Product Designer at Facebook

With the above quote and my previous research, I began the design exploration with two questions in mind related to individual's privacy and reputation management on social media.
1. What is it like to follow the lessens I found?
2. How can I give users more control without cluttering the sharing experience?
In order to answer these questions, I created a number of designs and prototypes using Framer to test and guide my concepts. The chapter documents my selected design application, Social Media Filter.

7. Charlie Deets. "Design for Privacy on Facebook – Facebook Design." Medium. September 5, 2014, https://medium.com/facebook-design/designing-for-privacy-on facebook-5b62e3f8e631#.nvm624qy5.

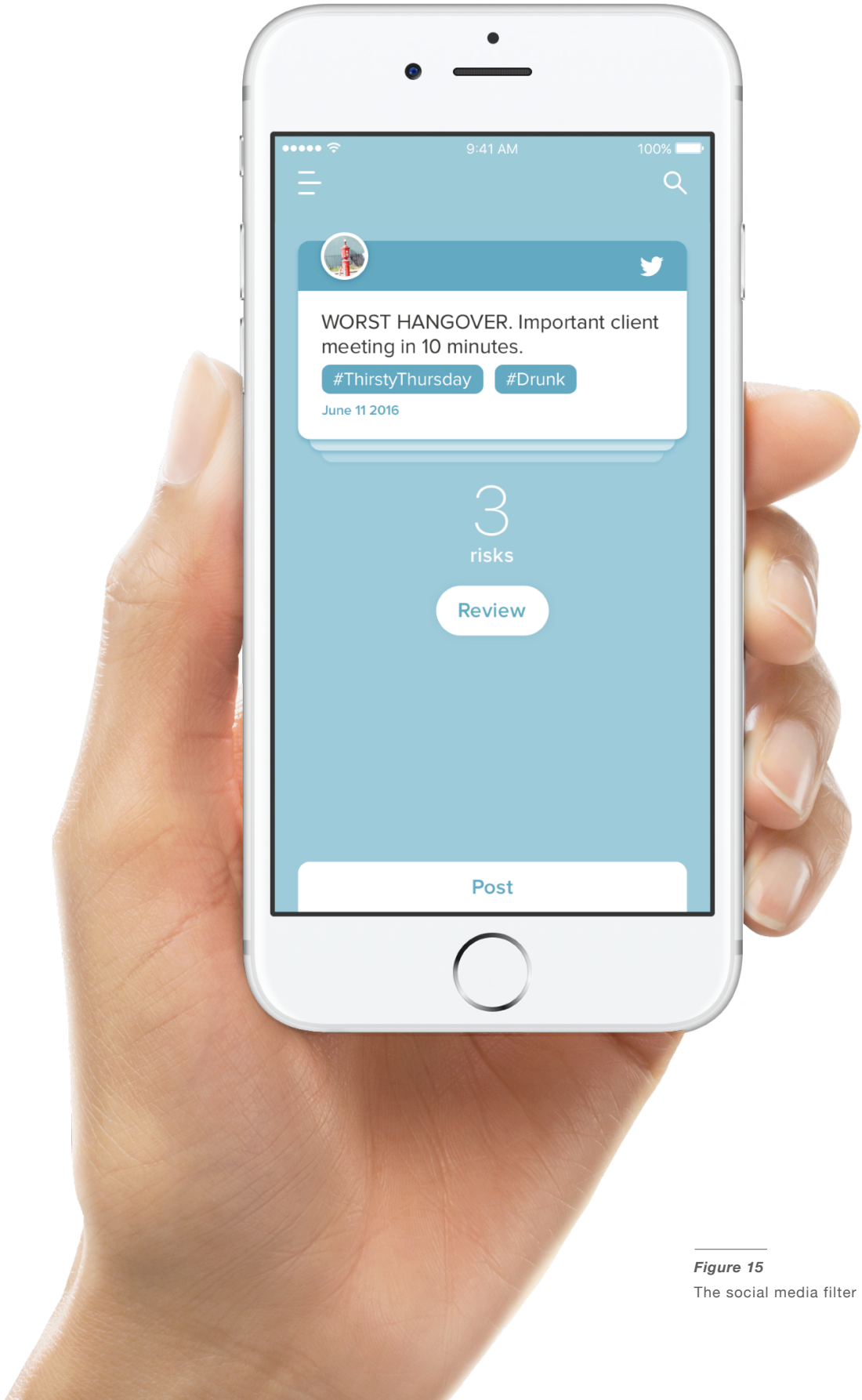


Figure 15
The social media filter

Social Media Filter, Lisa

The selected design application I propose for social media companies is an independent mobile platform with its own AI, Lisa, to mediate individuals and social media sites like Facebook, Twitter, and LinkedIn. Lisa is an intelligent personal assistant on smartphone, designed to improve the experience of managing your online privacy and reputation. By scanning separately all the content a user have shared and the content the user is about to share, Lisa can preemptively assesses any potential risks and consequences before a user posts to social media. Based on this assessment, Lisa then makes recommendations for how the shared content could be edited or how the new content could be posted, such as specifying selective audiences, level of visibility, and any triggers within images or text, providing you peace of mind even in the very moment when sharing online is about to take place.

In order to best communicate how Lisa would help people better manage their privacy and reputation on social media, I created two prototype vides demonstrating one possible storyline of the platform's use for the videos. The following session explains key functionalities Lisa provides.

Figure 17
A mediator between individuals and social media sites

Figure 18
The 'Link your social media accounts' screen

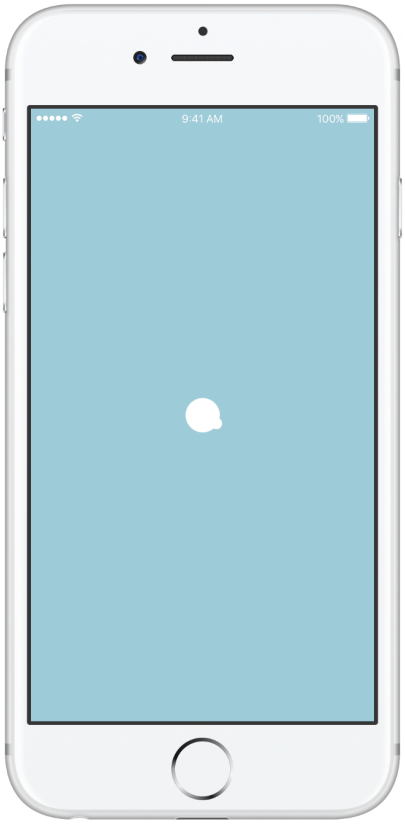


Figure 19
Loading screen

Linked Social Media Accounts

When the user downloads the app and signs in, the user can link their social media accounts by tapping each social media icons, since they are already logged into their social media accounts on their phones by saving their passwords on their devices.

Responsive Learning

Lisa can constantly learn about new changes in privacy policy and privacy settings of social media sites for the users. This way, the users do not need to keep an eye on these changes and study them.

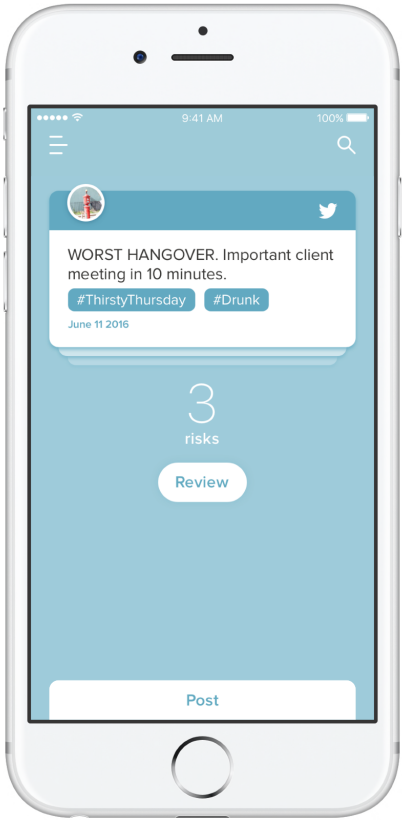


Figure 20
The filtered risks to be reviewed on the main screen

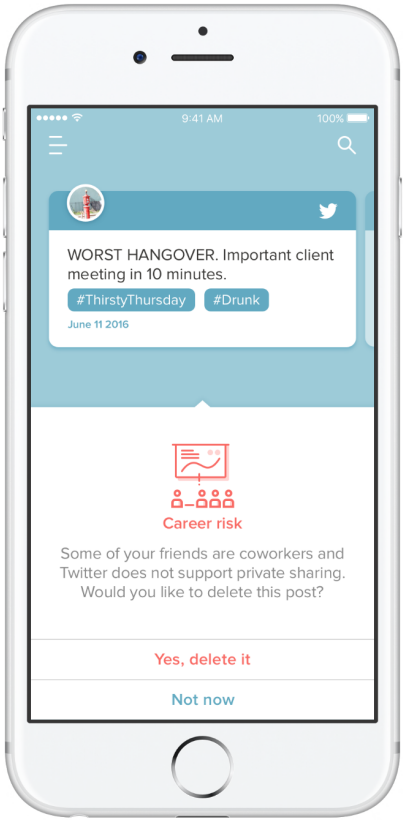


Figure 21
An example of filtered risks and recommendations

Filtering Risk

Once the social media accounts are linked to Lisa, Lisa automatically starts filtering out any potential risks from the users' old posts on the linked social media sites. Here are the examples of risks Lisa can find. Lisa then gathers the filtered risks for the user's review. When the user taps the 'review' button, the risky posts are spread out horizontally, pulling up recommendations, letting the user knows why it could be risky and how to eliminate potential risk factors. This way, the users does not need to read and assess every single posts they have shared on their social media sites.

Figure 22
Scanning a new content to assess risks before sharing

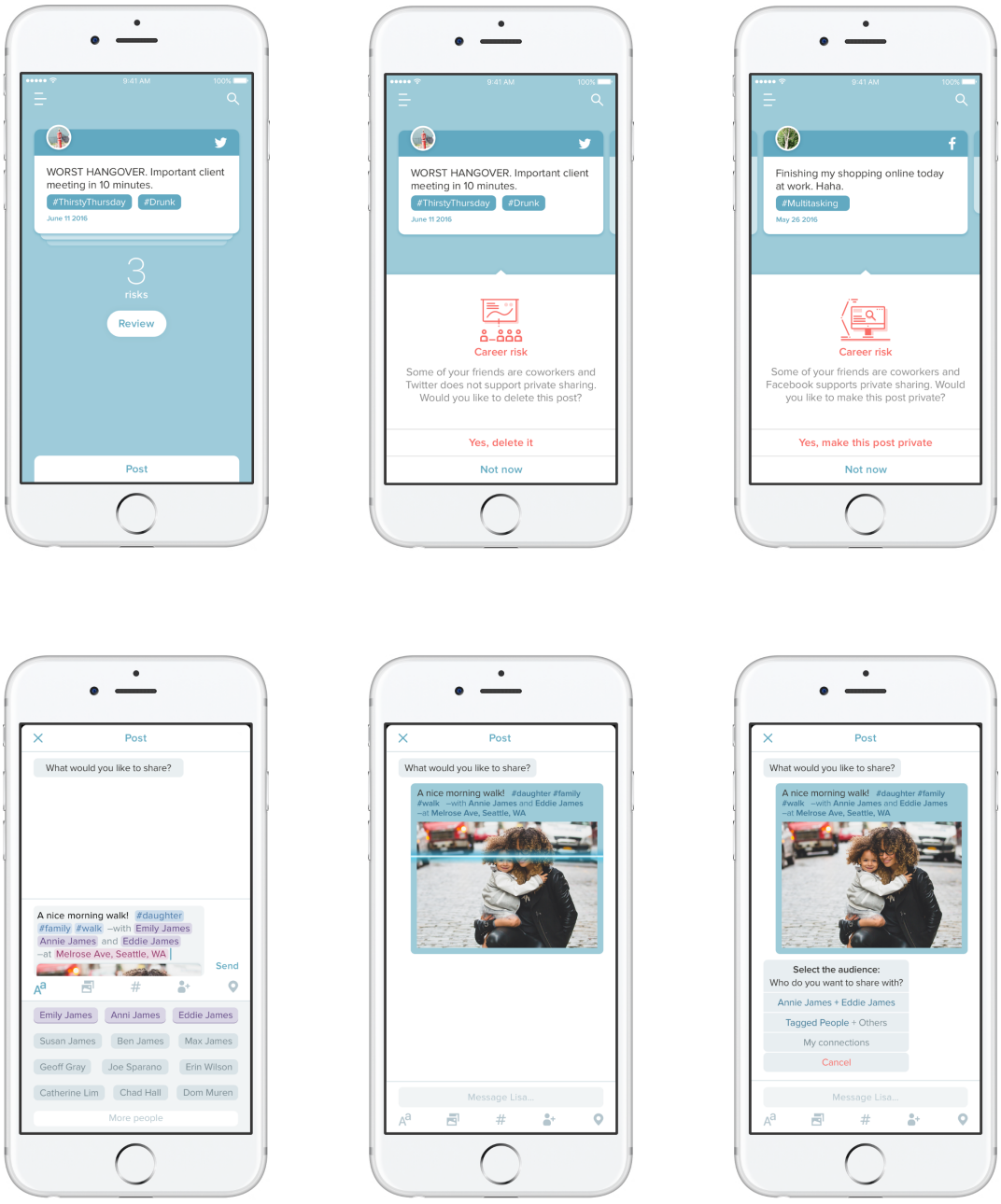
Figure 23
Making a recommendation to limit the audience

Posting Recommendations

Posting Recommendations: New content can be posted by messaging Lisa. Lisa suggests tags based on what the user types, people and location to tag based on the photo the user selects. Once the user message Lisa the content the user wants to share, Lisa preemptively accesses any potential risks and consequences before the content gets published on social media for the world to see. Based on this assessment, Lisa then make recommendations for how the content could be posted, such as specifying selective audiences, level of visibility, and any triggers within images or text, providing you peace of mind in the very moment when sharing online is about to take place.

Figure 24
'Sign Up' process

Figure 25
Managing old content (middle) and new content (bottom)



AI is changing the way people mange data.

Technological Feasibility

Since social media filter, Lisa, is a concept project that heavily relies on Artificial Intelligence (AI), the feasibility of this project depends on development of AI's cognitive learning and natural language processing. IBM's Watson is a well known example of the natural language processing technology. IBM describes Watson as a cognitive computing that uses natural language processing to find answers and reveal insights from large amounts of data, including news articles, research reports, and social media posts.[8] According to another article 'IBM's Watson is learning its way to saving lives' by Jon Gertner on FastCompany, it can read more data in a day than any human could in a lifetime, and keeps learning without forgetting a fact.[9] A recent article by Sam Byfold on The verge, IBM is trying to make Watson to see images analyze them.[10] Even though Watson has been pushed toward health care industry, it is capable of the fundamental things this project requires: understand the natural language, read social media posts, find certain types of things, and provide insights.

As a result of the recent huge success of Amazon's Eco, many people expect AI to change the way people search things online and interact with devices. However, I believe that it would change the way they manage their privacy and personal information in the near future. Therefore, I am optimistic about the feasibility of this project.

8. "What is IBM Watson?". IBM. http://www.ibm.com/smarterplanet/us/en/ibmwatson/what-is-watson.html.
9. Jon Gertner. "IBM's Watson Is Learning Its Way to Saving Lives." October 15, 2012. Fast Company. http://www.fastcompany.com/3001739/ibms-watson-learning-its-way-saving-lives.
10. Sam Byford. "After AlphaGo, What's Next for AI?" March 14, 2016. The Verge. http://www.theverge.com/2016/3/14/11219258/google-deepmind-alphago-go-challenge-ai-future.

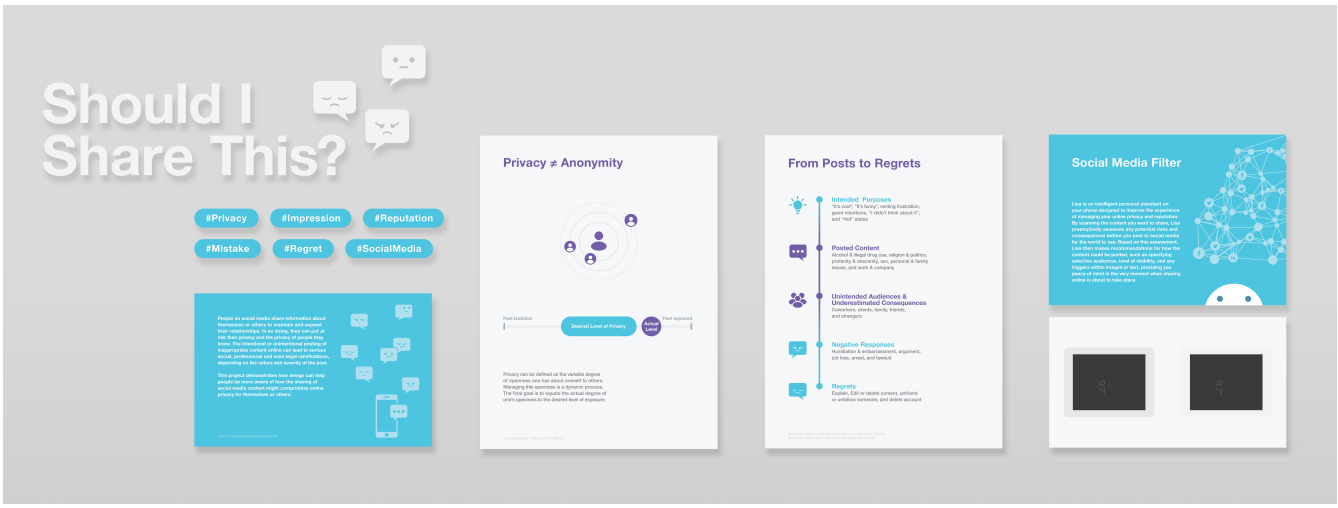
The Henry Art Gallery

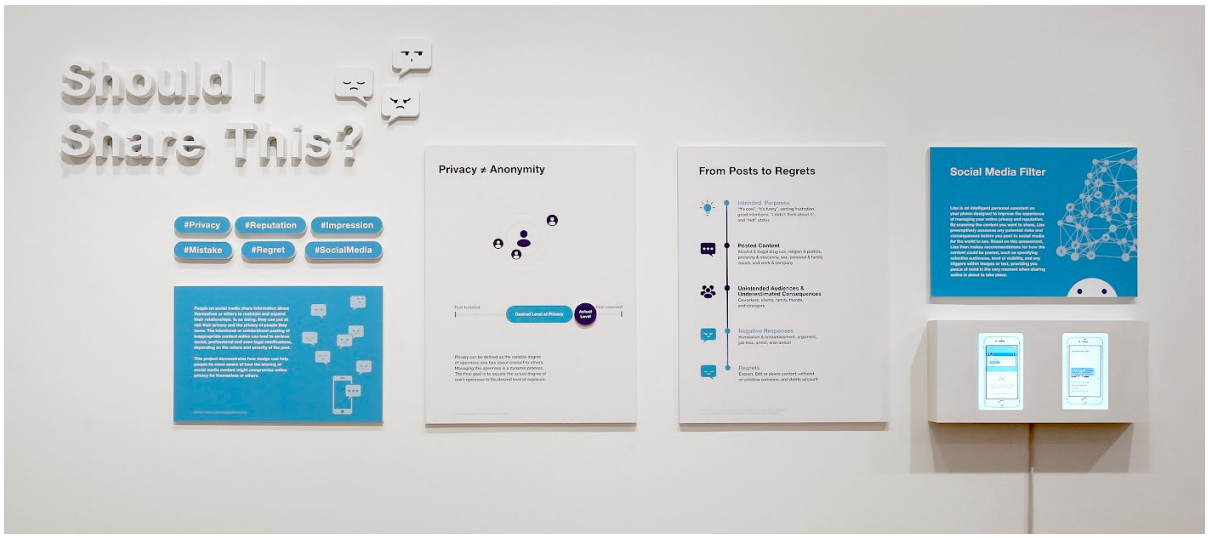
Figure 26
The exhibit entrance taken by Mark Woods

The Exhibition

In addition to the final designed product for the thesis, I spent a couple of weeks to think through how I would display my work at the Henry Art Gallery and another couple of weeks on the production of materials and their installation at the gallery from the end of April to the end of May. Transforming my project into a gallery setting in such a short time presented some technical difficulties, but I designed my space to leave the essence of each phase: what this project is about, what privacy is, why people make privacy mistakes, and what I propose. The following images documents the process of planning, making, and installing.

Figure 27
The process of planning (middle), prototyping (bottom left), and making (bottom right) for the the henry exhibit





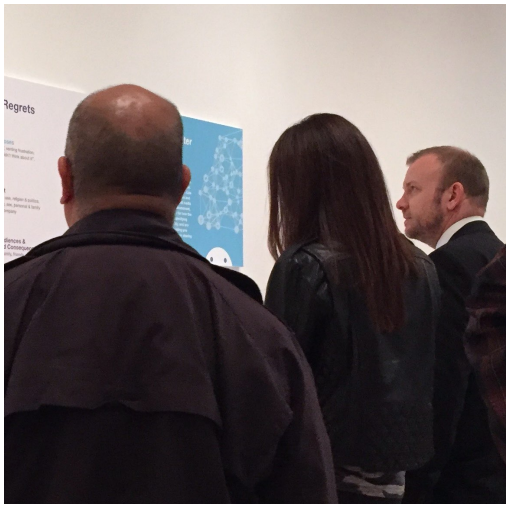


Figure 28
The finished exhibit installation taken by Mark Woods

Figure 29
The engaged audience

Many people are concerned about their privacy,

The Defense Presentation

The thesis defense presentation took place in the Husky Union Building on June 3rd and each presenter allotted for 20 minutes including the Q&A session for the audience. Few seconds after I finished my presentation, more than two third of the audience raised their hands to contribute their opinions about this project, which demonstrates the high level of audience engagement in this research. Due to the time constraints, I was not able to hear from each of the audience members who raised their hands, and I suspect that not all of them would agree on the way I approach the final visualization. The important thing here is that it proves that privacy is an issue that all of us can relate to.

However, I discovered that there are a plurality of attitudes people have about privacy. Among several questions raised during the Q&A session, one audience said “as an employer, I’d like to see these posts more and actually I would encourage them to post something like that.”, as a response to the first example of what Lisa could filter. Even though I defined privacy as the shifting level of visibility one desires regarding one’s personal information to others during my presentation, it may not sound clearly emphasized to some of them. Privacy is not about what others want to see, it is about what individuals feel comfortable sharing regarding their own personal information. Nobody has the right to see someone’s personal content without their agreements and permission. In February, there was a huge arguments about whether Apple should help FBI break into terrorist’s phone or protect users privacy, but Apple decided not to because it violates their rules for user privacy.[11] In addition, personal sharing on social media is declining,

11. Ellen Nakashima. “Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks.” The Washington Post. February 17, 2016, https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903eed4d9-11e5-9823-02b905009f99_story.html.

but still want to engage with what others post.

even though people are spending more time on social media. It seems clear now that many people are concerned about their privacy but still want to engage with what others post.

When it comes to privacy, anyone can have different opinions and various levels of comfort, and they all make different judgements on one's personal information when they see it. However, it is not about telling absolute right from wrong. Privacy can also be defined as a right of freedom not to be judged by others in unexpected and wrong ways.

Reflection

One meaningful insight I gathered about privacy while working on this project over the past nine months is that people's notion of privacy is contextual and dynamic, rather than being absolute and static. This insight originated from the poster session that was held last December. At the time I was looking to define what privacy is on social media and how it can be defined. Hoping to get closer to the answer, I put a board alongside my informational poster that asked people two questions: "Considering the spectrum of privacy (the spectrum, explained in the informational poster, includes identifiable data, 'like' data, behavioral data, communication data, and location data.), are you comfortable with sharing all of this information on social media?" and "If you are informed that you will be watched by someone in any given moment, what are the things you are comfortable doing?". I placed stickers besides my board for people to answer these questions. From participant responses, 27 people answered for the first question and 40 people answered for the second one. Their answers were varied, and some of these included answers for the first question like the

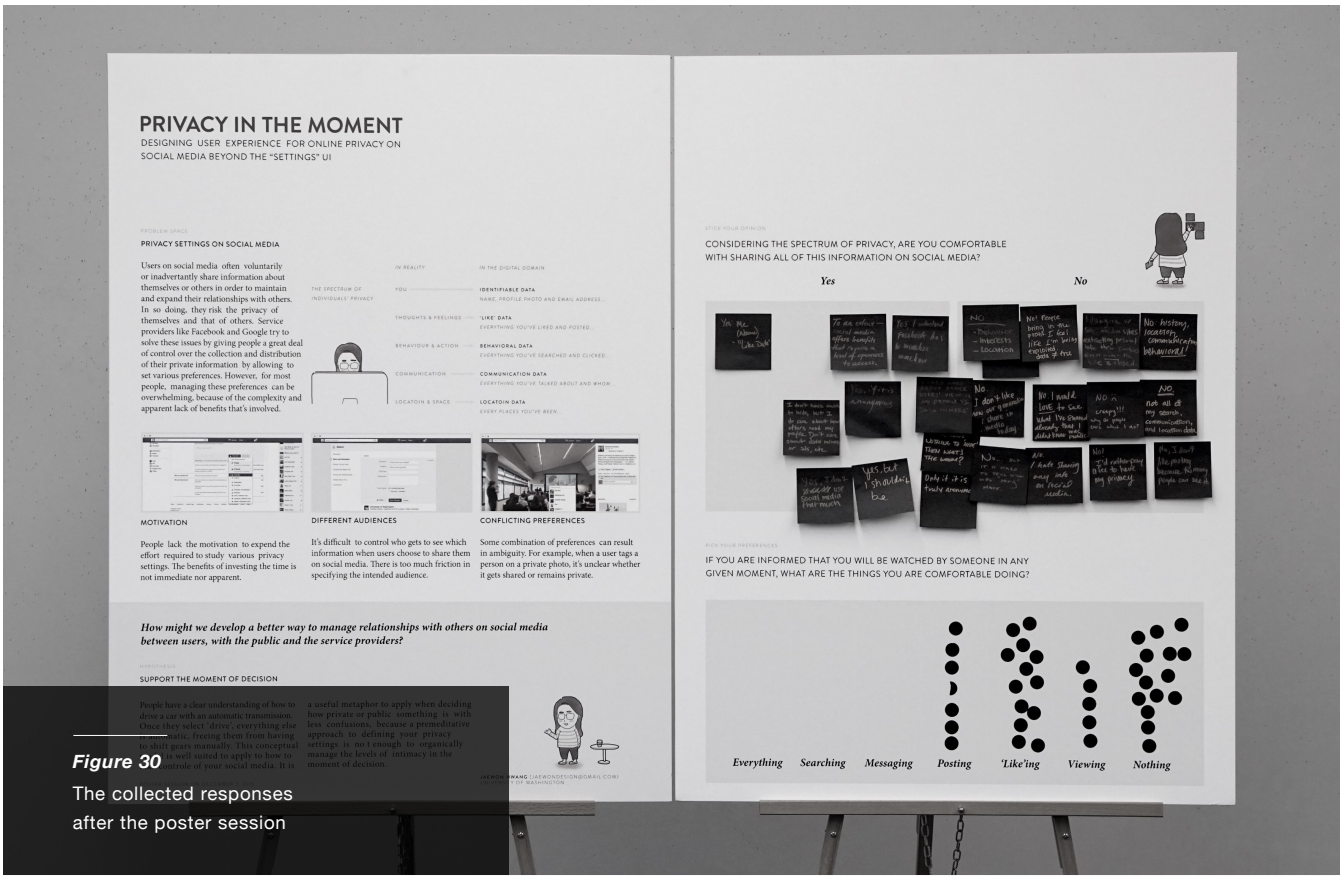


Figure 30
The collected responses after the poster session

following: “Yes, I don’t have much to hide. But I do care about how others read my profile. Don’t care about data.”, “Yes, I don’t use social media that much.”, “Yes, if it is anonymous.”, “Only if it is truly anonymous.”, “No behavior, no interests, and no location.”, and “No, not all of my search, communication, and location data.”. For the second question, 15 people said they are comfortable doing nothing if they are watched by someone. Additionally, 5 people said viewing and 13 people said ‘like’ing. Lastly, 6 people said posting and 1 person expressed their ambivalence for by tearing a sticker in half and putting it on the board. What does this mean? Looking back, at the past few months, now the answer to this question seems clear. Many people expressed conditional yes or no to the first question. And the person who answered with half a sticker also expressed the conditionality of their comfort. They needed to know what information and what content is going to be shared with whom, because privacy is contextual and we make privacy decisions based on many determining factors.

Many people expressed conditionality of their comport.

Conclusion

The world is becoming more connected as a result of the growth of ubiquitous computing models. In this trend towards any and all information about everyone and everything being accessible at the tap of a button or with a simple gesture, is it even possible to design with User Privacy first? In a lot of ways, designing for privacy first runs counter to the encouragement of desirable user behavior; sharing everything all the time and engaging what other users are sharing. However, I hold the belief that individual privacy is a fundamental right of any human being and it is worth protecting. This belief led me to take on the challenge of designing a social media product that gives users more control over what they share.

So I started this project by reviewing a number of journals, surveys, and web articles about individuals' privacy both in the physical and digital worlds in many different disciplines like computer science, social physiology, law, and philosophy. It helped me in defining what individuals' privacy is in the physical world, why they manage their privacy, and how it could be applied in the digital world. Then I moved on to a case study of how social media products support users' privacy and all the tasks they actually do within and beyond the Settings in order to manage their privacy and reputation online. It led me to discover important issues in Settings and privacy preferences, importance of specifying selective audience, and other tasks individuals do in order to better manage their privacy and reputation on social media. Based on these research findings, I began an iterative design process.

One of the things that design can achieve is balancing ideas, incentives and motivations that seem inherently opposed to each other. In this project, the core challenge was giving users more control without cluttering the sharing experience. But at a larger level, I realized that my project was really about removing the underlying concerns that people have when using social media products; sharing too much and compromising the privacy of themselves and others they know.

Two months ago in April, I read an article by Sarah Frier 'Facebook wants you to pst more about yourself' on the Bloomberg blog. The article wrote that people share less about themselves on Facebook, because of privacy concerns, especially due to the difficulties involved in selecting audience based on the context of content they are going to share. By designing for these concerns I believe that we can arrive at a win-win situation where people feel safe sharing more and more online. Social media service providers only stand to benefit from increased engagement from users that feel safe.

Thesis Documentation

Thank you all.

Acknowledgements

I would like to thank the following people who helped support this project and provided honest feedback over the past nine months:

My committee:
Jason O. Germany and Dominic Muren, and Sang–gyeun Ahn
MDes colleagues of 2016:
Catherine Lim, Chad Hall, Joe Sparano, Geoff Gray, and Erin Wilson
UW faculty:
Linda Norlen, Annabelle Gould, Karen Cheng, Tad Hirsch, Axel Roesler, Kristine Matthews, and Christopher Ozubko

Lastly, special thanks to my family for their encouragement and patience throughout this project.

Sources

Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press 2008.

Kerr, Ian, Valerie M. Steeves, and Carole Lucock. Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society. Oxford: Oxford University Press, 2009.

Altman Irwin. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Brooks/Cole Publishing Company, Monterey, California, 1975.

Goffman, Erving. The Presentation of Self in Everyday Life. Garden City, NY: Doubleday, 1959.

Schlenker, Barry R. Impression Management: The Self-concept, Social Identity, and Interpersonal Relations. Monterey, CA: Brooks/Cole Pub., 1980.

Nissenbaum, Helen. "Privacy as Contextual Integrity." Forthcoming: Washington Law Review, 2004.

Vinsel, Anne, Barbara B. Brown, Irwin Altman, and Carolyn Foss. "Privacy regulation, territorial displays, and effectiveness of individual functioning." Journal of Personality and Social Psychology 39, no. 6 (1980): 1104.

Wang, Yang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Lardinois, Frederic. “Google Teams Up with Harris Interactive to Launch New Self–Service Consumer Research Tool.” Tech Crunch. September 18, 2012, http://techcrunch.com/2012/09/18/google-harris-interactive-market-research/.

Faith Cranor. ""I Regretted the Minute I Pressed Share"" Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11, 2011.

Anne Gammon. “Social Media Blunders Cause More Damage to Important Relationships Today than Two Years Ago.” YouGov. July 22, 2015, https://today.yougov.com/news/2015/07/22/social-media-blunders-cause-more-damage-important-/.

Deets, Charlie. “Design for Privacy on Facebook – Facebook Design.” Medium. September 5, 2014, https://medium.com/facebook-design/designing-for-privacy-on-facebook-5b62e3f8e631#.nvm624qy5.

Frier, Sarah. “Facebook Wants You to Post More About Yourself.” Bloomberg. April 7, 2016, http://www.bloomberg.com/news/articles/2016-04-07/facebook-said-to-face-decline-in-people-posting-personal-content.

Gertner, Jon. “IBM’s Watson Is Learning Its Way to Saving Lives.” October 15, 2012. Fast Company. http://www.fastcompany.com/3001739/ibms-watson-learning-its-way-saving-lives.

Sources

Nakashima, Ellen. “Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks.” The Washington Post. February 17, 2016, https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee d4d9-11e5-9823-02b905009f99_story.html.

Perrin, Andrew. “Social Media Usage: 2005–2015.” Pew Research Center. October 8, 2015, http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

Liam Stack. “Egyptian Aviation Student Who Made Trump Threat Is Leaving U.S.” The New York Times. March 7, 2016, http://www.nytimes.com/2016/03/08/us/egyptian-aviation-student-who-made-trump-threat-is-forced-to-leave-us.html.

Byford, Sam . “After AlphaGo, What’s Next for AI?” March 14, 2016. The Verge. http://www.theverge.com/2016/3/14/11219258/google-deepmind-alphago-go-challenge-ai-future.

Vozza, Stephanie. “How to Avoid Social Media Regret” Fast Company. October 13, 14, http://www.fastcompany.com/3036936/the-future-of-work/how-to-avoid-social-media-regret.

“What is IBM Watson?”. IBM. http://www.ibm.com/smarterplanet/us/en/ibmwatson/what-is-watson.html.

Koshy, Vinay. “61+ social media facts and statistics you should know in 2016” Sprout Worth. http://www.sproutworth.com/social-media-facts/.