User-to-User Privacy in Social and Communications Applications

Camille Cobb

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

Doctor of Philosophy

University of Washington

2019

Reading Committee:

Tadayoshi Kohno, Chair

Alexis Hiniker, Chair

Ryan Calo

Program Authorized to Offer Degree:
Paul G. Allen School of Computer Science & Engineering

University of Washington

Abstract

User-to-User Privacy in Social and Communications Applications

Camille Cobb

Co-Chairs of the Supervisory Committee:
Professor Tadayoshi Kohno
Paul G. Allen School of Computer Science & Engineering

Professor Alexis Hiniker
Information School

Many people use social and communications applications that routinely expose potentially private information to friends, family, coworkers, and even strangers. This dissertation focuses on the interpersonal or "User-to-User (U2U)" privacy risks and concerns that arise in social and communications applications. I identified that U2U Privacy considerations are particularly relevant in the context of online dating, which I studied through a survey of 100 online dating users, follow-up interviews with 14 survey participants, and direct observation of 400 Tinder profiles. I found a wide range of potential information leakage channels, user practices, and privacy expectations in this specific application class. For example, Online Status Indicators (OSIs), which I observed in several online dating applications, represent one facet of online self-presentation that users may want to control. Many apps besides online dating apps also have OSIs — including Facebook, Instagram, and Google Hangouts. To expand our understanding of U2U Privacy issues beyond the specific context of online dating, I performed an analysis of the OSI design space across 40 applications from diverse app genres, and I surveyed 200 people to understand how OSIs affect their engagement with social and communications apps. I found that OSIs lead to app-dependent behaviors (*i.e.,* when users contort their behavior to meet the demands of an app). A theme that emerged

as particularly relevant throughout this work is that many design choices affecting U2U Privacy represent nuanced trade-offs between privacy and other user goals, privacy for one group of users versus another, or competing aspects of privacy. To enable app designers and future researchers to study these trade-offs more broadly, I have developed a methodology called "Would You Rather" that encourages users to directly consider and express preferences related to technology.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

This dissertation is the culmination of many years of work, during which I have received invaluable guidance and support in all aspects of my life, both professional and personal, from many people.

First, I am incredibly grateful to my thesis advisors Tadayoshi Kohno and Alexis Hiniker. Yoshi saw potential in my abilities at a point in my graduate school experience when I felt particularly lost, and he has never failed to provide encouragement and support. I am especially thankful to Yoshi for giving me the freedom and encouragement to explore research directions that I was passionate about. I greatly admire Alexis' knowledge and perspectives — she often points out meaningful aspects of my work that had not yet considered. Working with Alexis during her first years of being a professor has helped me more concretely envision a similar career path for myself, and I will undoubtedly look back to the examples I have gained through her example of how to mentor students, structure courses, and do research. I also thank Ryan Calo and Ted Mack for being part of my dissertation committee and providing helpful feedback on my dissertation research.

Before I knew Yoshi or Alexis, I had other mentors and advisors at UW who have had a profound impact on my life. I owe it to David Notkin that I chose to come to UW at all, which I believe has been an incredible blessing. During visit days, David made it clear that he would support and mentor me in finding a research direction that I cared about, even if that meant helping me find a different advisor. Gaetano cared deeply about his students, about the world, and about the positive impacts of his work; my time working with him showed me that I can have a successful career in this field while prioritizing the people around me and focusing my research on topics that are good for the world. I am grateful that I was able to

know David and Gaetano and wish that they had been able to see me achieve a more stable footing in grad school.

As I made my way to the Security and Privacy Research Lab, I explored many other research and industry possibilities. Throughout this exploration, I am thankful to have felt a sense that, although I did not always have an advisor or research direction, I was surrounded by faculty who cared about my success and happiness. I especially want to thank Mike Ernst, Richard Ladner, Dan Grossman, Anna Karlin, and Richard Anderson for showing this support explicitly by checking in on my progress over the years. I also want to thank Kate Starbird who helped me explore my research interests, gave me opportunities to mentor undergraduate and high school students in research, and helped me earn the NSF Graduate Research Fellowship. I would additionally like to thank Elise Dorough, Lindsay Michimoto, Sophie Ostlund, and Mel Kadenko Kurt Schwehr hosted me as an intern for my first two summers during grad school on Google's geo-oceans team. This internship experience actually made me reconsider whether I should stay in grad school because it felt like exciting and meaningful work and demonstrated to me that I could find fulfillment outside of academia (which has been a huge comfort when grad school becomes stressful), but I am nevertheless thankful for the experience, because it helped me be confident that I have made a truly active choice to pursue this degree and career path. I owe a great deal of thanks to several people in particular who helped me decide to pursue a PhD in the first place. My undergraduate advisor Sara Sprenkle provided me with my first research experience, and taught me to love asking and answering questions that contribute new knowledge to the world. Lori Pollock and Lori Clarke took me on as an undergraduate researcher during two of my summers as an undergraduate student.

I am thankful to my colleagues in the Security and Privacy Research Lab. In particular Lucy Simko, for her friendship, support, and the joy it has brought me to collaborate with her on research, which actually started while we were in undergrad together. I also collaborated

with undergraduate researchers in the security lab — Kayla Butler and Clemend Zhong who both did excellent work. I am also thankful to the greater lab community, including Christine Chen, Alexei Czeskis, Tamara Denning, Ivan Evtimov, Earlence Fernandes, Gennie Gebhart, Chris Geeng, Karl Koscher, Kiron Lebeck, Ada Lerner, Shrirang Mare, Peter Ney, Temitope Oluwafemi, Mitali Palekar, Franzi Roesner, Kimberly Ruth, Lucy Simko, Anna Kornfeld Simpson, Ian Smith, Alex Takakuwa, and Paul Vines. It has been amazing to belong to the community within this lab. Being part of the Tech Policy lab has helped me make more meaningful research contributions and taught me about impacts of technology on the world that I might not have learned about otherwise. At earlier points in graduate school, I was also welcomed into other communities — the PLSE and ICTD Labs and my original office in CSE. I am thankful to my fellow students in those groups for collaborating with me on coursework and providing me with a sense of community when I was in a new place. In particular, Nicki Dell and Waylon Brunette provided feedback to help strengthen my NSF GRFP application, and acted as peer mentors early in my PhD.

Outside of research, people I met or got to know through extracurricular activities have profoundly improved my experience at UW and in Seattle. I am especially thankful to Professor Juliet McMains for renewing my excitement about social dance by teaching the history and social context of dances as well as technique, for supporting me in learning the 'lead' role, and for starting conversations about consent on the dance floor. I am also thankful to my teammates playing soccer, softball, and inner tube basketball over the years, and to my dance instructors and partners.

My closest friends in Seattle are a group of people I hope to stay close with forever, even as many of us graduate and scatter away from Seattle: Aleks Holynski, John Toman (and Laura and Corvin Toman), Ryan Maas, Joe Redmon, Jeff Snyder, Doug Woos, and Daryl Zuniga. Finally, I would not have been able to pursue a PhD without the support of my family — especially my mom, Dawn Cobb, and my dad, Ronald Cobb.

DEDICATION

To my dog Stormy, who has helped me get through and enjoy the last five years in more ways than I can say. She reminds me to get outside, eat, go to sleep at a semi-reasonable hour, and laugh, and she's always willing to listen to my practice talks.

Chapter 1
INTRODUCTION

As new social and communications technologies gain popularity, users navigate frequently changing and sometimes confusing interpersonal features of applications they use. Social norms and behavioral expectations for interacting with other users and their sometimes private information are complex and vary between applications, social groups, and over time. Along with the emergence of new social and communications applications, novel privacy risks have also surfaced. In this dissertation, I will focus on the ways in which users of popular social and communications applications may violate each others' expectations of privacy and how users work to maintain their privacy in these apps. A recurring theme throughout my work is that users face nuanced, complex trade-offs related to their privacy. People who design and regulate technology should understand these trade-offs in order to develop technology that supports users' privacy preferences and goals rather than requiring them to adapt their behavior and expectations to suit a tool's features and capabilities.

1.1 User-to-User Privacy

I refer to between-user privacy as **"User-to-User (U2U) Privacy."** U2U Privacy is consistent with and builds on prior work on "interpersonal privacy" (*e.g.,* by Patil et al. in 2011 [93]). I use the term U2U Privacy because it highlights a specific thematic focus of this dissertation. Namely, while interpersonal privacy includes social consequences of technical privacy breaches (*e.g.,* marital strife after hackers leaked user information from Ashley Madison — an online dating service for people seeking an affair [107]), my focus on U2U Privacy stresses that privacy concerns arise even in the absence of technical vulnerabilities, or skilled, powerful, or specially privileged adversaries (*e.g.,* hackers, government actors, or

advertisers). U2U Privacy describes situations that occur between between typical users — with average technical capabilities (or who are at least not leveraging their technical skills to gain access to information beyond the app or service's UI) and without special permissions or privileges that could allow them access to privileged user data. These situations can include concerns about information leakage, efforts to control one's online self-presentation, and intentional or unintentional access to or monitoring of another user's information that the other person did not anticipate (*i.e.,* privacy violations). The typical users I have described may be strangers, or they may know each other. Although people may have more trust and willingness to share certain information with people they know, like friends, family, neighbors, or colleagues, there are also many more motivations for a preference to keep certain information private. People who know each other may also be able to make informed inferences based on socially-gained knowledge. Security and privacy literature often refers to "targets" and "adversaries." Referring to the actors in U2U Privacy scenarios as fellow users emphasizes that anyone can be a target or an adversary at any time. Thus, I rarely refer to users as adversaries or targets and instead describe how people may *act* adversarially or may *experience* privacy concerns or violations. In the context of adversaries such as government actors, hackers, or invasive companies, it might make sense to have a one-sided, risk averse view of privacy. But considering U2U privacy requires a different, more nuanced perspective, because although people want to protect themselves from other users, conscientiously sharing private information about oneself is how people grow closer and build relationships.

1.2 Research Questions

My dissertation explores two fundamental research questions:

- **RQ1: How and why do users disclose private information to other users, and how do users interact with information about other users that apps make available to them?**

- **RQ2: How are these disclosures influenced by design, and how can designers**

bring these disclosure behaviors in line with user preferences?

In this section, I will describe how each of these overarching research questions is addressed in my dissertation.

1.2.1 RQ1: Practices and Preferences Related to Information Disclosure

This research question entails many specific sub-questions, which more closely informed the methodological structure of my studies (*e.g.,* the questions and prompts in surveys and interviews):

- What information do users disclose online to other users (possibly without wanting to, or without realizing or actively deciding to do so)?
  - In my study of privacy in the context of online dating (Chapter 2), I took two approaches to understanding what information users disclose in their online dating profiles. First, I asked participants in a survey to specify which information they choose to include in their profile. Second, I analyzed the contents of Tinder profiles, considering only whether they disclosed their employer, educational history, and whether they had linked their Instagram account to their Tinder account. I found that many users share relatively non-sensitive information such as their name and photo that would nevertheless be sufficient to identify them based on their profile, which may lead to privacy violations based on how other users choose to interact with this data. Many survey participants also noted sharing potentially sensitive details about themselves such as their sexual orientation, sexual preferences or kinks, sexual history, and more.
  - In my exploration of Online Status Indicators (OSIs) (Chapter 3), I focused on a specific type of information that users inevitably share with others if they use certain apps. I found that almost all participants in my survey regularly use at least one app that conveys this online status information to others. Prior work

shows that online status information can be used to infer other, potentially private, information about a user [37], and participant responses to my survey reinforce the potential for online status information to be a vector through which someone might infer secondary information that is more sensitive than the online status itself.

- What motivations do users have for disclosing certain information (especially if their choice to disclose that information is in conflict with their sharing preferences) or keeping certain information private?

  - In my study of online dating, survey and interview participants discussed wanting to convey a sense of their personality, values, hobbies, etc. in their profile. A primary reason for using dating apps is to find a compatible match, and participants described how information disclosure in their profile could help or hinder them in this goal. For example, participants who choose to be more private in their profile may find that other users do not trust that they are a "real person" or might find that they are unable to filter (or be filtered by others) such that the people they communicate with are likely to be compatible matches.
  - Related to OSIs, participants in my survey described both beneficial use cases for OSIs, in which they might *want* to disclose their online status, and situations in which they did not want to appear as online, to negotiate interpersonal interactions with others (*e.g.,* avoiding unwanted conversations).
  - In both of these studies, I found that the choice of whether or not to disclose certain information to certain people involves a trade-off for the user. The Would You Rather (WYR) methodology I have developed (Chapter 4) can help illuminate some of these motivations. For example, the WYR scenario "Would you rather have no matches [in an online dating app] or 100 matches you aren't interested in?" which was written by separate participants from the original online dating

study, draws attention to the user goal of trying to find compatible matches that was a theme in the online dating surveys and interviews.

- Who do people care about sharing or not sharing information with?
  - In both my study of online dating privacy preferences and users' experiences with OSIs, people were especially cognizant of information that would be shared with or seen by their employers or coworkers, family members, and romantic partners. In some cases, participants were more eager to share information with people they know in these capacities. For example, some people felt that OSIs are especially useful and relevant in a business context so that they could reach out to ask questions and expect a quick reply. However, many participants in my online dating study wished to avoid seeing their coworkers' profiles and having their profile seen by coworkers.

- What expectations do users have about how others will behave in relation to the information that they share (intentionally or unintentionally, consciously shared or passively broadcast)?
  - In my survey related to online dating, I asked participants directly about certain behaviors such as taking screenshots of other users' profiles or looking people up online before (or after) a date. I asked participants if they engage in these behaviors, how common they believe these behaviors are in general, and how they would feel to learn that someone else treated their profile in these ways. I found that there was a wide range of responses and beliefs about the etiquette around these sorts of behaviors, which can lead to violations of users' expectations of privacy.
  - In the technical analysis of OSI designs, I considered how a variety of designs affected the ability of a motivated adversary to track someone's OSI longitudinally

and make inferences about their behavior. Though not asked directly, participants did not seem to anticipate that anyone would realistically engage in such focused monitoring of their online status. Nevertheless, participants encountered broken expectations in terms of what they thought others might notice or what actions they might take based on their OSI (*e.g.,* one participant was surprised to be called out by a colleague for regularly playing video games late at night).

1.2.2 RQ2: How Design Influences Disclosure

Again, it is useful to break this high-level research question into specific sub-questions that are answered more directly in the research I present in this dissertation. Though many of the findings related to these specific sub-questions suggest that in addition to technology design, disclosure is influenced as much or more by pressures from other users or an inability to control or predict the behavior of other users. I assert that, at least to some degree, app design that is considerate of these interpersonal factors could lead to apps that better support users' disclosure preferences.

- What leads users to unintentionally or unknowingly disclose information about themselves?
  - In the interviews I conducted as part of my online dating research, participants' main experiences related to accidental information disclosure were related to difficulties controlling or anticipating the audience of their profile. Participants also surfaced concerns related to how *other users* might (mis)use the information they disclosed, for example by taking screenshots of their profile and sharing them in other online forums such as on Reddit or in Facebook posts.
  - In my work related to OSIs, I learned that users might accidentally take an action that causes them to appear as online. For example, by asking participants whether they realized that apps they use regularly have OSIs, I found that many

participants were not even aware that some apps they use have OSIs at all. Design that makes this feature more noticeable to users could help avoid inadvertent disclosure.

  - In one WYR case study, discussions with participants brought up the relevance of being able to *anticipate* that information about you will be disclosed. For example, the WYR scenario "WYR have a microphone listening to you all the time or a camera recording you all the time?" prompted participants to inquire "Well, do I know it's happening?" This suggests that although one of these monitoring techniques may leak more sensitive information in their typical daily life, they may have felt more capable of *controlling* either their visual or verbal self-presentation, and it might, therefore, be preferable to choose the option that offers more control.

- What influences users to disclose information about themselves *despite* their information disclosure preferences?

  - Online dating users described how their goals for using the app (*i.e.,* finding a compatible romantic match) influenced them to disclose potentially sensitive information (*e.g.,* sexual preferences). Similarly, direct or perceived pressure from other users influenced some participants to share more than they would have otherwise. This perceived pressure was sometimes related to a sense of obligation to reciprocate others' sharing choices. For example, participants described how access to identifying information could help engender trust before meeting a stranger in person, and since they wanted to be able to look up their dates online, they felt that they should also disclose enough to make this possible for their matches. Dating apps could be re-imagined to support those user goals without necessitating that users automatically disclose sensitive or identifying information to all other users who see their profile.

  - Reciprocation also played a role in users' choices to share their online status; however, this was directly influenced by app design in some cases. Several apps that allowed users to turn off their own OSIs prevented users who had done so from seeing others', even if they were shared willingly, which could lead to a coercive scenario in which users decide to share their own online status in order to continue seeing others'. Many apps with OSIs, however, did not allow users to turn off their OSIs at all — it is impossible to access those apps without disclosing that you are using them. In these apps, users face the trade-off of not using the app at all or disclosing their online status and may sometimes choose to use the app despite this undesired disclosure.

- Can and do users "exploit" social features to learn secondary information about other users? Do they do so with malice, or for some other reason? How do users feel about or cope with such actions on the receiving side?

  - In my study of online dating, I found a wide range of expectations around the etiquette for appropriate interactions with the information that others had disclosed in their profile. For example, while the majority of participants in my survey thought that it was common and acceptable to look people up online based on the information in their profile, this was *not* universally agreed-upon, and participants shared a wide range of beliefs about what look-up behaviors were acceptable (*e.g.,* just searching for them on Google versus using a reverse image search of their profile photos). Thus, users would likely disagree about what constitutes an "exploit," but I did learn that many users *do* engage in behaviors that others would see as invasive.
  - In my survey focused on OSIs, I was surprised to find that many participants described uses of OSIs (by or against them) that could contribute to abusive relationships or other problematic interpersonal situations. For example, participants described OSIs being used to detect cheating in romantic relationships, to learn

if colleagues or employees were working efficiently, or to learn whether a friend was angry at or avoiding them. In some cases, participants made these sorts of inferences although they were not necessarily aiming to be adversarial (*e.g.,* passively noticing someone's OSI), but many participants also described opening apps *specifically* to look up someone's online status and/or described scenarios that must have represented someone taking active steps to surveil others via their online status.

1.3 Related Work

While this dissertation is not the first or only work that addresses the questions I posed in Section 1.2, it strives to be a systematic analysis of these questions in the context of one domain (online dating) and one type of information leakage channel (OSIs). In particular, some of the earliest work in the area of Usable Security and Privacy identified aspects of system design that hindered users' ability to achieve security and privacy goals [109], and subsequent research has shown that design influences users' security and privacy behaviors in other contexts as well (*e.g.,* in the context of browser warnings [55]). Das *et al.* found that social factors can also influence users' security and privacy behaviors [45].

Related to understanding the causes and impacts of privacy violations in social media, prior work related to privacy in social media apps — including Facebook [24, 48, 70, 74, 75, 91, 101], Twitter [77, 85], and Snapchat [97] has revealed evidence of users misunderstandings about permissions, misuse of others' information, and social, physical, and financial risks resulting from privacy breaches. Other studies have explored how factors such as what information is being shared, at what granularity, with whom, and the broader context influence users' privacy preferences [32, 33, 69, 73] (*e.g.,* in the case of sharing location information, *where* the user is, the time, and who they are with could influence whether they are willing to disclose their location to a specific other user). The Platform for Privacy Preferences Project (P3P) sought to give users more control of what information they disclosed to websites or other online services [44]. Despite these efforts to better enable users to achieve their

privacy goals, researchers have surfaced the ways that designers use "Dark Patterns" to trick users — often in ways that violate their security and privacy preferences [3, 40, 53]

Although I have studied online dating and OSIs, U2U Privacy implications exist in the context of other types of apps and social features as well. Tensions related to information shared between users via typing notifications, Instagram's poll feature, Strava, Facebook's "suggested friends" feature, and Venmo have received attention in popular culture and/or research [14, 21, 68, 38, 78]. Though it has not been portrayed it as a U2U Privacy concern, several studies have found that various aspects of the content users post on social media (*e.g.,* the colors in their Instagram photos) correlate with mental or physical health conditions (*e.g.,* depression) [96, 112]. It may seem unlikely that other users would seek to track and analyze their friends' posts to infer this type of sensitive information, but it nevertheless represents a possible information leakage channel, and I *did* find that users observe OSIs to learn whether their friends are okay or safe. Situations that fall under U2U Privacy also emerged in research studying the instances where users feel a sense of panic or embarrassment related to their privacy [25, 27, 49]. Highlighting the role that competing user goals have in users' privacy choices, Meng and Zuo found that too much privacy (*i.e.,* the inability to connect with strangers) contributed to the messaging application QQ's popularity over MSN messenger in China [86].

Chapters 2, 3, and 4 each contain a related work section that addresses additional work pertaining to the specific topics explored in that chapter. That is, Chapter 2 highlights additional prior research that has focused on users' experiences in the context of online dating. In Chapter 3 I consider research related to online status, digital traces more generally, patterns of app use, and users' experiences with messaging apps. In Chapter 4, I discuss other research on developing human-centered, collaborative methodologies, use and analysis of ipsative measures, and how phenomena related to social conformity and the Privacy Paradox may factor into our understanding of data collected with the WYR method.

1.4 Thesis Overview

In Chapter 2, I focus on U2U Privacy in a specific application domain — online dating. Online dating services let users expand their dating pool beyond their social network and specify important characteristics of potential partners. To assess compatibility, users share personal information — *e.g.,* identifying details or sensitive opinions about sexual preferences or worldviews — in profiles or in one-on-one communication. Online dating profiles are typically visible to wide audiences of other users, which may include both strangers and acquaintances, coworkers, or friends. I present the results of a survey of 97 online dating users, 14 semi-structured follow-up interviews, and structured observation of 400 Tinder profiles. Although many participants were dismissive of their own privacy concerns, they easily recalled instances in which they had felt tensions or experienced violations related to their privacy. Examining participants' responses collectively, I found a wide range of expectations regarding what participants felt were acceptable ways to interact with information in other users' online dating profiles (*e.g.,* whether it is acceptable to look someone up online and the degree of depth that is acceptable for this). My results reveal tensions between privacy and competing user values and goals, and I demonstrate how these results can inform future designs of online dating services.

Through my focus on online dating, I identified that specific app design features may act as a channel through which potentially sensitive information is revealed to other users. One such feature is Online Status Indicators (or OSIs, *i.e.,* interface elements that communicate whether a user is online). OSIs exist in several online dating apps but are also implemented in popular apps of other app genres. By studying OSIs (Chapter 3, I have demonstrated that U2U Privacy considerations exist in a variety of app genres, and that the privacy challenges or violations that users encounter extend across the boundaries of a single app or type of app. I analyzed 184 mobile applications to characterize the existing design space of OSIs and identified 40 apps with OSIs across a variety of genres. I describe common patterns in the design of these OSIs, including variations in appearance, visibility to others, and OSI

settings, finding, among other things, that less than half of these apps allow users change the default settings for this feature. I also survey 200 smartphone users to understand the extent to which they are aware of the information they passively share via OSIs and how they feel about this. Despite their familiarity with OSIs, participants misunderstand many aspects of OSIs, and they describe expending substantial cognitive effort to curate and control their self-presentation via OSIs. Some users further report that they leverage OSI-conveyed information for problematic and malicious purposes. Drawing on the existing constructs of *app dependence* (*i.e.,* when users contort their behavior to meet the demands of an app) and *app enablement* (*i.e.,* when apps enable users to engage in behaviors they feel good about), I demonstrate that current OSI design patterns promote app dependence, and I call for a shift toward app-enabling OSI designs.

My studies of U2U Privacy in the context of online dating and OSIs have shown that users and app designers face nuanced, complex trade-offs between privacy and other user goals, privacy for one group of users versus another, or competing aspects of privacy. To enable app designers and future researchers to study these trade-offs in other application domains or relating to other types of technology or design features, I have developed a methodology called "Would You Rather" that encourages users to directly consider and express preferences related to technology. "Would You Rather" was originally designed to elucidate user concerns, values, and preferences related to the trade-offs they face while using technology; however, it can also be adapted to specifically focus on generating or evaluating novel design ideas in the context of these user values and preferences.

1.5 Contributions

My dissertation offers several contributions, both specifically in the application domain of online dating and relating to OSIs and broadly in terms of our collective understanding of U2U Privacy:

- My surveys and interviews of online dating users offer a **broad understanding of**

users' experiences, preferences, and strategies related to privacy in the context of online dating.

- My analysis of 400 Tinder profiles reveals **ground-truth evidence of what users disclose in their online dating profiles and how information disclosure influences the ability of others to look them up online.**

- My analysis of 40 applications with OSIs provides a **typology of how OSIs are designed across a variety of app genres.**

- My survey studying users' experiences with OSIs helps us understand **ways that specific design choices impact users**, and **evidence of how users navigate and cope with passively broadcast information disclosure in the context of a variety of interpersonal relationships.**

- The WYR methodology contributes a **novel approach to studying trade-offs that users face while using a variety of technologies**.

- Collectively, my dissertation surfaces **themes related to privacy trade-offs** and **best practices that can help guide designers to creating technology that better enables users to control their online self-presentation to other users**.

Chapter 2

A BROAD EXPLORATION OF USER-TO-USER PRIVACY IN A SPECIFIC APPLICATION CLASS: ONLINE DATING

In this chapter, I present a research study focused on privacy concerns in the context of online dating. In this work, I found that users face trade-offs between privacy and other goals they have for using online dating, such as finding a compatible romantic match. Participants conveyed a variety of U2U Privacy risks that they perceived or experienced while using online dating services. I identified mismatches in users expectations related to information disclosure in profiles, behaviors such as looking people up based on the information in their profile or taking screenshots of conversations and profiles. The work of this chapter previously appeared in a 2017 paper [41], and I conducted all of the work this chapter in collaboration with Tadayoshi Kohno.

2.1 Introduction

Online dating services enable users to connect and develop romantic relationships with other users who they might not otherwise meet. Past research has examined varied aspects of the online dating ecosystem, such as how people cultivate the impressions that they give others and how to provide a better user experience, *e.g.,* [81, 111, 113]. Much less attention has been paid to how users perceive, navigate, and manage privacy risks in online dating.

Online dating is a particularly unique domain because information in online dating profiles may be simultaneously *more public* (*e.g.,* accessible to a wider audience since users often aim to connect with people *outside* their social networks) and contain *more sensitive information* than profiles on other social media. Users may be motivated to include information, such as their sexual kinks and religious beliefs, that they believe will help them find a compatible

romantic partner yet might not share with people they know (*e.g.,* Facebook friends). This situation is in direct conflict with the goals of most permissions models. Recent high-profile events demonstrate that privacy issues in online dating deserve additional attention. For example, during the Rio Olympics, a Tinder user took screenshots of Olympians' profiles and posted them publicly on social media [19]; subsequently, a journalist used Grindr to collect identifying information about closeted gay Olympians [84].

My focus on privacy is multi-fold. First, I seek to understand users' perceptions about and actions governing their privacy. For example, I seek to assess users' level of concern about their own privacy, the reasons for their concern or lack thereof, and how these concerns manifest in online dating behaviors. Additionally, since privacy involves multiple actors (the party who has information to share or keep private, and the party who might intentionally or accidentally learn that information), I study the reciprocal side of privacy: how users consume (possibly) private information from and about others. I leverage a combination of methods to achieve these goals: a survey, follow-up semi-structured interviews, and an analysis of Tinder profiles. A key contribution of my work is a portrait of existing user practices and views surrounding privacy in online dating. From this, I identify explicit tensions and challenges (presented inline with results) and give suggestions for how online dating system designers can better support user goals, including privacy (Section 2.11).

2.2 Online Dating Overview

I now review online dating services, focusing on two that were most discussed in the survey responses — OKCupid and Tinder; I then broadly discuss others. A 2016 report says that 15% of Americans have used online dating — three times the number who had used it in 2013 [1]. Tinder generates 26 million matches per day [10]; OKCupid claims over 1 million app installs per week [7]. I describe the services as they exist now but acknowledge that features change, and some survey participants used only previous versions (see Section 2.5).

Tinder. By default, a user's first name, age, gender, job, and education (if present) are imported from Facebook and displayed in Tinder profiles. Profiles also include photos and

text. When a user views a profile, they see mutual Facebook friends and the distance to the other user (based on the phones' GPS locations). Users may link their Instagram account to display recent photos and their Instagram username. Figure 2.1 gives an example (synthetic) Tinder profile.

Users view profiles in a queue called "Discovery." To view another profile, the user must "swipe right" to indicate a desire to connect or "swipe left" if they are not interested. Users have a limited number of right swipes per day. If both users swipe right, they "match" and may exchange messages and view each others' profiles at any time. Users select which gender(s) they are looking for and specify an age range and search radius. Users appear in queues only if they fit each other's search criteria. A paid subscription to "Tinder Plus" lets users "rewind" the most recent swipe, hide their age or location, "passport" to any location in the world (swipe as though they were there), and make their profile visible only to those they right swipe.

OKCupid. OKCupid profiles consist of: (1) a unique username, (2) demographic information, (3) text in suggested paragraphs, such as "What I'm doing with my life", (4) photos, (5) answers to multiple choice questions, many of which concern sensitive topics such as sexual history or preferences, religion, and drug use, and (6) a personality assessment based on answers to (5). Examples of (5) and (6) are shown in Figure 2.2. Questions also determine a "match percentage" with other users. By default, users answer questions "publicly," and answers become visible to others who answer the same question; "privately" answered questions influence match percentage and personality.

Users can view the profile of and send messages to other users unless they have been blocked. By default, users can see who has viewed their profile since their last login; they can browse covertly but cannot monitor who views their profile while they are "invisible." Users receive a notification if they mutually "like" others. A paid subscription to "A-list" lets a user see everyone who likes them and browse invisibly while retaining the ability to see who visits their profile.

Other Dating Services. Many general-purpose online dating applications exist, some

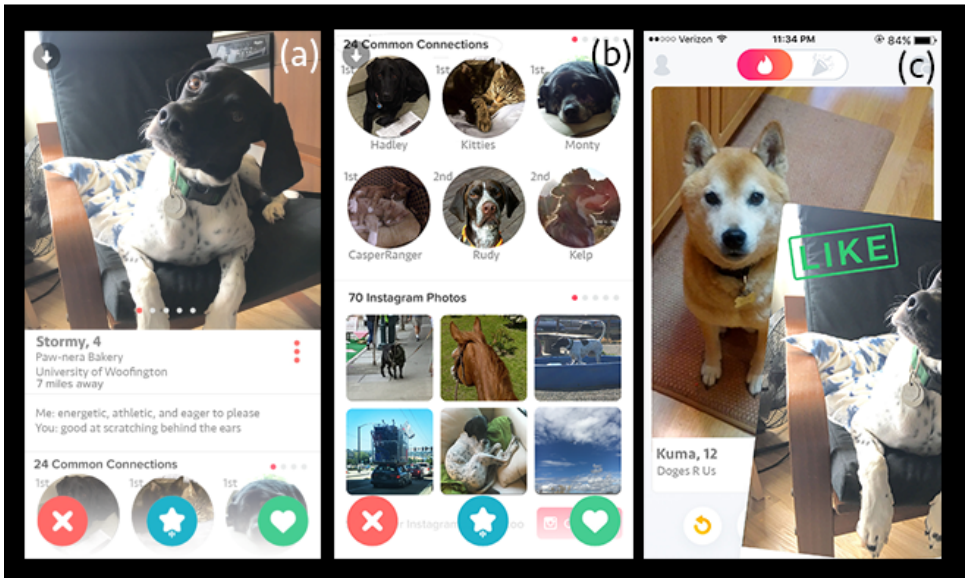


Figure 2.1: Example Tinder profile (generated in Photoshop, not a real user) in (a), scrolled down in (b); right swiping reveals the next profile (c).

Figure 2.2: Screenshots showing OKCupid's personality assessment (a) which is based on answers to questions, like the one in (b).

with features or designs that pose potential privacy implications. Coffee Meets Bagel gives users only a handful of profiles to evaluate each day and displays users' first names only if matched. The League leverages users' LinkedIn accounts to block coworkers. On Bumble, women must initiate conversations, and matches expire if no messages are exchanged within a specified time frame. Other online dating services — like Grindr, JSwipe, and Christian-Mingle — cater to specific demographics.

Although they did not surface in this study, third-party applications may break users' expectations. For example, Firetind claims to let Tinder users browse profiles with no queue and see *everyone* who right swipes them.

2.3 Context and Related Work

Privacy, online dating, and recent high-profile incidents. The media has covered data breaches and vulnerabilities in online dating systems. For example, online dating sites Ashley-Madison [107], PositiveSingles [17], and HZone [100] were targets of breaches that divulged identifying data, and association with those sites revealed that users had considered an affair, had an STD, or had HIV (respectively). Researchers have found, for example, that dating apps exposed sensitive past in-app messages [54] and allowed precise geolocation of users [94]. I do not consider the effects of technical vulnerabilities in this work.

Recent events emphasize the importance of understanding how users' privacy expectations can be violated by other users: researchers released sensitive and identifying information about 70,000 users by creating an account to scrape OKCupid [9], screenshots of Olympians' Tinder profiles were shared publicly on social media [19], identifying information from closeted Olympians' Grindr profiles was published by a news site [84], and news has also covered stories about online dating users experiencing physical violence or stalking [18]. In these examples, in contrast to data breaches, authorized parties (with accounts) caused harm by violating users' expectations and trust.

Online dating research. Several past studies have also focused on privacy in online dating. One study [60] used data collected in 2006 — when Facebook was relatively new and

the iPhone had not yet been released — and found a statistical correlation between online dating users' concerns about personal security, misrepresentation, and being recognized by someone they knew and "uncertainty reduction behaviors" (*e.g.,* looking someone up, saving messages, and asking follow-up questions of the other user). The researchers additionally note that their results do not explain the high degree of variance in participants' responses. A more recent survey of Wellesley College students who use Tinder [102] asked participants what privacy meant to them and if they considered it to be important. They also looked at 30 Tinder profiles to determine if people can be re-identified from their profile. In my analysis of Tinder profiles, I begin with the same question, but for a larger population, and study not only whether users can be re-identified from their profiles but also what properties affect identifiability (Section 2.10). Additionally, compared to both works, the surveys and interviews in this work take a qualitative approach to understand a wide range of issues and include participants who have used a variety of online dating systems at some point during a relatively long time-frame (2001 to present).

Within the online dating ecosystem, other research has explored a broad range of topics, such as: whether people portray themselves accurately [65, 104], impression management [113], how people leave online dating systems [36], and how users are successful at online dating [81, 111]. A line of related work focused on understanding Grindr users' preferences and desires in online dating, *e.g.,* [34, 43, 63, 106]. Although privacy was not the focus, because of its importance, privacy considerations surfaced in some of these studies.

2.4 Methods

This research combines three methods, all approved by the University of Washington's IRB: (1) an open-ended survey, (2) an analysis of Tinder profiles, and (3) semi-structured interviews with a subset of survey respondents. Survey responses informed the design of Tinder profile analysis, and both surveys and profile analysis informed the structure of follow-up interviews.

Because the surveys provided an initial glimpse into privacy preferences and practices

and interviews let me delve more deeply into those same issues, I present survey and interview results together, followed by the results of my Tinder profile analysis. Despite this presentation order, my Tinder analysis results contributed to the interview design. Further, I stress that the goal is not to provide comprehensive, quantitative, generalizable results over all online dating systems and populations, but rather to consider a diversity of populations and systems with the goal of uncovering unique challenges and lessons.

2.4.1 Survey

Survey contained 24 multiple-choice, 15 open-ended, and 10 demographic questions [8]. I designed the survey using an iterative process, informed by my own experiences with online dating, feedback from colleagues, and small-scale pilots. The survey remained open throughout the duration of this research, though most responses were collected prior to Tinder profile analysis and interviews. I recruited participants by posting a link to the survey on public forums and by propagating it through both researchers' social and university networks (*i.e.,* snowball sampling).

Survey questions addressed respondents' general use of online dating and their experiences, practices, expectations, and feelings about disclosing information, looking up other users or being looked up, taking screenshots, and the intersection of real-world and online encounters. I intentionally did not define privacy and instead let users surface the concerns that are most relevant to them.

Demographics. The survey received 99 total responses, of which I included 97.[1] I excluded two responses: one person had not used online dating, and one submitted the form twice. Table 3.4 summarizes study demographics.

51 participants had used online dating for at least three months of the past year, while 28 had not used it at all in the past year. 60 started online dating in 2012 or later. 66 use or previously used OKCupid; 44 use or previously used Tinder (and an additional 17 tried it).

[1]Percentages out of 97 are similar to the raw numbers of respondents, so I do not include the percentages.

Age	20-24 (18), 25-29 (44), 30-34 (16), 35-39 (9), 40-44 (3), 45-49 (4), 50-55 (3)
Education	High School or GED (2), Associate Degree (4), Some College (6), Still in College (3), College or More (82)
Ethnicity	White (68), Asian (10), Hispanic (3), Black (2), Other or Unspecified (14)
Gender	Male (35), Female (61), Unspecified (1)
Occupation	Student (26), Teacher (9), Computer Engineer (7), Other or Unspecified (55)
Relationship Status	Single (50), Seeing Someone or Married (37), Divorced, Separated, or Widowed (7), Open Relationship (2), Unspecified (1)
Religious Views	Christian (36), Atheist (17), Agnostic (12), Jewish (7), Other or Unspecified (25)
Sexual Orientation	Straight (83), Bisexual (6), Gay or Lesbian (4), Other or Unspecified (4)

Table 2.1: Summary of survey participant demographics

Use of 27 additional dating services was reported by participants, and 65 participants tried at least 3 online dating services. 44 reported that it was common or very common to use dating services amongst their friends; 15 said it was uncommon or very uncommon, while 38 were neutral.

2.4.2 Tinder Profile Analysis

To gather ground-truth insights about profiles' content and findability (defined below) to supplement self-reported participant information, I created two Tinder accounts associated with Facebook accounts for a 26 year-old man and a 26 year-old woman and used these to analyze content from 400 Tinder profiles: 100 26 year-old women (men) seeking men (women) in Seattle, and a corresponding number in Atlanta. 26 year-olds are well-represented in online dating [2] and old enough to have employment histories. Atlanta and Seattle represent cities with different demographics. I chose Tinder because it is popular and has the convenient property of its queue dictating an order in which to consider profiles. Tinder's "Discovery" settings specify which profiles will appear in a user's queue, but only allow users to specify their own gender and the genders of people they prefer to match with. At the time of this study, Tinder presented only binary gender choices. Users are only shown to each other if they mutually meet each others' Discovery criteria. Thus, a person on Tinder who is a man can only see profiles of people who are interested in matching with men, even if his settings convey an interest in people of all other genders. In order to avoid including the same profile in the analysis twice *(e.g.,* a bi or pan person could appear in the queue for both the male and female research profiles), I needed to restrict each of the two accounts to only viewing one gender. I chose to consider only women (men) looking for men (women), because this is the most common demographic. Additionally, since this part of the study did not include an informed consent step, I felt that it was important to minimize the potential negative impacts of research that studies potentially private information about people from marginalized groups.

To minimize possible effects on queue ordering, I used new (blank) accounts, swiped

only left, and viewed profiles during the day on weekdays. Per the IRB's request that I not interact with other users or collect identifying information, I used settings that prevented others from seeing the research profile unless I swiped right, which I did not; I was also careful never to record identifying information. All searches were in a private browser, and I did not use reverse image search, which would involve saving profile photos.

Our team collaboratively conducted pilot data collection to refine and systematize data collection and search procedures. We delineated both steps that we would take and steps that we would explicitly not take to look someone up. This process allowed me to develop a consistent, uniform approach for data collection. I collected the final data and both researchers participated in data analysis.

Defining "found." I marked a profile as "found" if: (1) I found their last name, (2) I found additional account(s) of theirs or page(s) with information about them, *and* (3) I was sure it was the same person. This is likely an overly restrictive definition of finding someone, and searching would be easier without the constraint of never saving identifying information and using new accounts with no friends. Hence, these results offer a rough lower bound on users' searchability.

Data collected. For each profile, I recorded: (1) if I found the person, (2) if found, if their Tinder photos were found elsewhere, (3) if their job and/or school were listed, (4) if their Instagram was linked or if usernames for other accounts were listed, and (5) how unique their first name was according to howmanyofme.com.

2.4.3 Interviews

I conducted 14 semi-structured phone interviews, each lasting up to an hour, with survey participants who consented to follow-ups and responded to interview requests by my internal cutoff date (seven men and seven women). My own experience with online dating informed my perspective in these interviews, and my identity as a woman may have influenced how comfortable participants felt discussing dating-related topics with me. I audio recorded the interviews with participant consent; both researchers participated in analysis, including

an affinity diagram exercise to identify themes in surveys and interviews. Informed by survey results and Tinder profile analysis and leveraging the semi-structured nature of the interviews, I probed further into topics surfaced in surveys and additionally discussed why users chose particular dating services, use of paid features, and perspectives about recent privacy-violating events related to online dating (Section 2.3).

2.5 General Results

I begin my analysis by focusing first on general observations, then turning to in-depth discussions of specific topics (Section 2.6–2.9). I combine survey and interview analyses in Section 2.6–2.9 and discuss Tinder profile analyses in Section 2.10. Note that survey and interview data were self-reported and may reveal the union of a participant's practices on multiple services.

Motivations for using online dating. 62 survey respondents' goal for online dating was dating or marriage; 20 hoped to date and make friends; 13 sought casual sex in addition to friendship and/or dating; one was exclusively seeking platonic relationships; one wanted to "see what's out there"; no one reported using the service only to find casual sex partners. Participants also reported using online dating for entertainment, to get over an ex, "to think about who I want to date," (P41, F, 21, interview)[2] or to "familiarise myself with a new area after moving" (P71, F, 26).

P73 (M, 27) compared it to a basic need: "eveybody [*sic*] needs the chance to get out their [*sic*]." P1 (F, 27) felt pressure to use online dating: "I feel like I need to meet people, then realize that I actually don't really like it and stop for a few months, then worry that it's hard to meet people otherwise anymore." On why she preferred online dating, P40 (F, 23) wrote, "We were introverts and we liked the ability to see people's interests and KNOW they were interesting [*sic*] in dating before speaking to them."

Though not addressed in the survey, interviewees gave the following reasons for choosing

[2](P41, F, 21, interview) denotes Participant 41 (after randomizing participant order), female, 21 years of age, and that the quote was from an interview and not the survey.

a dating service: their friends used it; it was popular; it was free; it had specific security or usability features; they had more success than with others; or they knew successful couples who met using it.

Reasons for stopping online dating. Mirroring reasons for choosing a dating service, survey respondents mentioned cost and lack of success as reasons they stopped using a service. 30 survey respondents stopped using online dating because they found a partner. Others got bored, preferred to meet someone offline, ran out of potential matches, did not like the messages they received, felt they required too much time, or became frustrated over scams or bots.

Related to privacy, P48 (F, 23) wrote, "It felt weird to know a lot about a person before meeting them." In contrast, two survey respondents stopped using services with limited profile space because "the apps generally had less information than I wanted" (P7, M, 33) and they "couldn't glean any actually useful info from any profiles" (P2, F, 22).

Paying for features. Although many participants preferred free online dating services, three (not asked directly) appreciated OKCupid's paid privacy features which allow users to specify (*i.e.,* whitelist) who may view their profile. Some users were not familiar with these options. For example, P80 (F, 24, interview) thought paying offered only a way to *boost* her profile's visibility rather than increase privacy. Current implementations of features on Tinder and OKCupid that allow users to whitelist audiences prevent users with similarly restrictive privacy settings from encountering each others' profiles. Facilitating connections between users who may be romantically compatible but have incompatible (or equally restrictive) privacy settings is a design challenge.

Impacts of demographic characteristics. These characteristics may influence users' experiences and perspectives on privacy in online dating. For example, P1 noted that young people were likely to be on their parents' phone plan and have a number with an area code, which reveals their hometown and makes them more searchable (Section 2.8). Users' locations when using these services could affect their privacy-relevant experiences. For example, P80 pointed out that because of gender imbalance in Silicon Valley, she was unlikely to encounter

her male friends' Tinder profiles. Likewise, because there are fewer women in the area, her male friends might be more likely to encounter her Tinder profile. Navigating privacy implications when different demographics are impacted differently is another challenge.

2.6 Perceived or Experienced Risks

To understand why users might be motivated to remain private (or not) in their profiles and what their internal threat models are, I highlight risks that participants anticipated or encountered using online dating.

Uncomfortable feelings. Awkwardness or embarrassment was a risk acknowledged by most participants, albeit often dismissively; however, it influenced how they used online dating services and is therefore an important consideration. 81 reported seeing the profile of someone they knew well offline, and 33 had seen a coworker's profile. 37 reported recognizing someone in public from their dating profile, and 30 coincidentally met someone in person shortly before or after seeing their online dating profile. Some had mostly positive feelings, noting that it was "kind of nice to know we're all in the same boat" (P93, F, 28), but others had a negative reaction: "I felt like I did something wrong, especially when I remember the app shows who has looked at your profile" (P68, F, 27).

Details remembered from profiles shaded some people's future in-person impressions: "It was one of those, I've totally seen that girl and remember her being really skanky online" (P73). Uncomfortable feelings were exacerbated if either user expressed interest: "It was also someone who had expressed interest in me who I wasn't interested in, so that was extra awkward" (P93). Sometimes the privacy of revealing only mutual attraction was appreciated: "I swiped right. They didn't do the same. All was well with no lingering curiosity" (P75, M, 30). However, this could be complicated because not everyone put the same care into swiping: "[My friends swiped using my account] with my consent but they would pick matches that I typically didn't like" (P65, F, 27).

Unanticipated disclosure. Online dating users may be unable to anticipate who will see their profile. Unanticipated disclosure can occur through data breaches, users sharing

information or screenshots (see Section 2.9), or other unexpected uses of the service. For example, users may not expect people to view profiles of people they are not interested in, as P94 (F, 36) did: "One time I was browsing other women's profiles just to get a sense of what the norms are in the online dating world (I'm a hetero woman), and I came across a friend's profile ... her profile made her seem emotionally unstable and batshit crazy." The impact of unanticipated disclosure varies; although P94's opinion of her friend may not have changed, in another case: "We discovered a friend's boyfriend was cheating on her, which led to the breakup of their relationship" (P71). I discuss strategies used to avoid unanticipated disclosure in Section 2.7.

Scams, bots, and catfishing. Concerns about scams, bots, and catfishing (*e.g.,* people presenting themselves as someone else through pictures and profile information) may affect users' privacy-relevant decisions. P76 (M, 26) aims to "Have a meaningful conversation with the person, so that I'm sure they're not some kind of scammer." P87 (M, 26, interview) was led on by a catfisher for several weeks and then threatened; he now takes the opposite approach: "I would never go after a girl that long without meeting them first." Each approach has its own risks — a meaningful online conversation could reveal sensitive information prematurely and with a written record, but meeting a stranger in person after only a brief conversation raises safety concerns.

After being asked if she was a bot because she did not disclose much in her profile, P89 (F, 27, interview) changed her profile to include where she went to school. As I discuss in Section 2.10, revealing one's school can affect privacy by making one more findable. A design challenge is how to enable P89 to convince others that she is not a bot while also not revealing more private information.

Although both men and women expressed concerns about these threats, two interviewees believed that men are at greater risk: "It does take presumably some work to create [fake accounts] and it's so much more likely to be successful as a woman. Dudes are so much more likely to swipe right" (P56, M, 27, interview).

Stalking, cyberstalking, inappropriate messages, violence. When asked why they

omitted certain information from their profile (free-response), nine survey respondents stated concerns about "creepy" people finding them or safety. People also felt relief or regret (depending on how the situation evolved) after revealing personal information to someone met via online dating, "I met someone once who turned out to live across the street and half a block down from me. Figured that out on the first date — good thing she wasn't nuts since she knew where I lived at that point ..." (P7). "After I did not choose to go on a subsequent date with someone, they found information about me online that I did not think was easy to locate, and they used this information to make me feel guilty. I was concerned the behavior might escalate" (P68). This participant explained later in an interview that she believed the person learned her last name when an iMessage was sent "from" her email address instead of phone number, used this to find her on Twitter, and followed links in her distant Twitter past to personal blog posts. This situation highlights the challenge that even if a person has certain privacy settings within their online dating app, other apps may leak private information.

Safety concerns might influence users to take actions that violate their own or others' privacy, such as informing friends about a date, looking up other users (Section 2.8), taking screenshots (Section 2.9), and asking a match for personal information (Section 2.7).

On the other hand, participants identified how online dating could empower users through mechanisms not available with traditional dating. For example, users can block people, exchange messages through the service until they feel comfortable exchanging contact information, and have sufficient information to "check up on" someone before going out with them. P41 saved messages to re-identify users who messaged her again after a long time and/or from a different account. To stay safe, some participants used strategies such as only meeting with someone who shares certain information (*e.g.,* a phone number) or if they are able to confirm their identity online or via mutual friends (see Section 2.8): "I usually wouldn't meet someone unless we have mutual acquaintances or I can find validating information about them online" (P11, F, 31). However, as discussed in Section 2.7, some users may wish to avoid sharing contact information or having a large online presence.

Employment and businesses. 65 survey respondents disagreed or strongly disagreed that it would be okay for an employer to use information from someone's online dating profile to make an employment decision, but only 36 felt the same way about public Facebook profiles. 12 survey respondents had seen the online dating profile of someone who worked in a public position at a business they frequented, such as a bartender, doctor, or instructor. Of the people who had this experience, nine changed their opinion of the person or the person's ability to do their job, suggesting that someone's online dating presence can influence users' impressions of businesses. Six participants said they preferred not to see and/or be seen by people who work at businesses they frequent. Participants who worked in public positions similarly expressed concerns about clients viewing their profiles: "I am a teacher and I was always afraid that my profile would be found by my students. I feel like anyone taking a screenshot would increase that likelihood" (P55, F, 26).

2.7 Disclosure of Information

Although some participants think dating services should prevent leaks, others believe users can prevent undesirable consequences: "I think one just has to be careful how many personal details they put online ... I think it could be possible to avoid security issues" (P31, F, 35). Indeed, some users did not worry about disclosure because they lacked "anything to be ashamed of" (P72, M, 27) in their profile: "if ... security is breached, I take comfort in my own profile's relative banality" (P35, M, 27). However, there are valid reasons to include potentially sensitive information in a profile, and even very basic information could be harmful if used in unexpected or malicious ways.

What people revealed in their profiles. I asked survey participants directly about content in their online dating profiles. 62 revealed their first name (only 8 revealed their last name); 45 revealed their job; 42 revealed their school; 38 had information about their sexual history or preferences; 64 revealed their religion; and 44 expressed political opinions or leanings. Only P42, a 39 year-old male who aimed to be "as private as possible," did not have a photo that included his face in his profile. 17 had photos that might be considered

sensitive (*e.g.,* of them drinking, wearing a swimsuit, in a sexually explicit position, or naked). Specific information participants withheld included their religion, name, job, school, physique, salary, and sexual preferences. When meeting in person, some were careful not to reveal their license plate or exactly where they lived.

How people chose what information to disclose. A dating service's design and default settings can influence what information users disclose. For example, Tinder requires users to display the name from their Facebook account, and OKCupid users must upload a photo before they can see more than a thumbnail of other users' photos.

Participants disclosed information to find more compatible matches; increase chances for a match; reciprocate when others share information; communicate their values, hobbies, sense of humor, and personality; or as a response to direct or perceived pressure from other users. Reasons for withholding information included safety, remaining anonymous, avoiding embarrassment, discouraging harassing messages (*e.g.,* not answering overtly sexual questions on OKCupid directly because of a perception that this leads to receiving more vulgar messages), controlling the way they present themselves to potential matches (*e.g.,* "I leave out the fact that I am bisexual, because it ... scares off both men and women" (P50, M, 28)), not being judged prematurely (*e.g.,* for living with his parents (P32, M, 28)), or because they did not consider the information relevant.

Interviewees wanted to get a sense of the character, interests, or other characteristics of potential matches. Rather than attributing it to privacy concerns, some users dismissed users who disclosed very little information: "If they don't have anything, I kind of skip over them because clearly they didn't put any effort into it" (P80). Some participants expressed a desire to learn specific information that others preferred not to disclose or had been pressured to reveal information they did not want to disclose (*e.g.,* job, socioeconomic level, apartment complex, full name, bra size, or phone number): "I dont [*sic*] like when people ask for my phone number, that's the limit" (P67, F, 29).

Some users noted internal tensions, realizing that, while uncomfortable to disclose, "things like names and locations are important to know when you're online dating ... and it's im-

portant to know that someone is employed" (P23, F, 29). I return to the privacy implications of disclosing employment in Section 2.8. P87 reconciled some of these tensions by modifying content rather than leaving it out completely, for example, by blurring logos or faces of friends in photos.

Selective disclosure. As discussed in Section 2.6, some users wished to selectively keep the fact that they are using online dating or information in their dating profile from some people (*e.g.,* friends, family, coworkers) while still making their profile available to potential matches. Beyond the paid features mentioned in Section 2.5, participants noted strategies to achieve (or approximate) this goal. P93, upon creating her account, "spent a whole day ... to find as many [people who work nearby] as I could and block them ... I missed somebody, inevitably." To minimize risk when using location-based applications, P68 reported: "I feel very uncomfortable when I see my coworkers' profiles, so I make sure to not use proximity-driven apps at work."

I did not identify direct concerns about someone actively trying to find users' profiles, but six participants used fake accounts or friends' accounts to covertly view profiles or send messages. 18 respondents acknowledged that, though they were unlikely to try, someone who knew them could probably find their online dating profiles. Others believed this would be difficult: "I think it would be very hard to 'find' it on purpose if they went out looking for it" (P94).

2.8 Searchability

This study surfaced a wide spectrum of views and practices on searching for information about other users.

Reasons to look people up. In surveys and interviews, users said that they looked up other users out of general curiosity, to find more recent photos, to be sure they were "real" people, to see if they were telling the truth, or to see if they had a criminal record: "I also liked it when [Coffee Meets Bagel] profiles included information that allowed me to Google someone ... I am extremely hesitant to go on a date without that information, because I

want to prevent sexual assault" (P28, F, 28). 58 survey respondents looked someone up when deciding whether to send them a message, respond to a message, or go out with them. 44 sought additional information after going on a date or agreeing to a date. 10 said they might look someone up if they caught their attention regardless of romantic interest.

What information was found. Based on information in their profiles, 77 survey respondents thought someone might be able to find their Facebook profiles. Although not asked directly, five participants offered that they would not want their Facebook to be found: "Facebook to me is very personal, basically an invitation to my life" (P31, interview). Participants reported finding other users' Facebook and LinkedIn pages, YouTube videos, other social media accounts, blog posts, and poetry.

How people searched. In surveys, five people explicitly mentioned using LinkedIn to search for people; 20 mentioned Facebook; and 19 mentioned Google. Survey participants also searched through Spokeo, court records, and other social media. I specifically asked about reverse image search, and 12 participants reported using it to find someone who reuses photos. Five people looked up someone's username on other sites, and four looked up a phone number. As a non-technical approach, 53 might ask a mutual friend.

Survey participants pointed out that finding information was easier with details such as name, location, phone number, occupation, or mutual friends: "If you know their name you can use Spokeo - if you know where they live and their name you can access State records like property tax records to see if they own a home" (P15, F, 51). P85 (F, 23) noted that inherent traits might make searching for them especially easy: "I have a fairly unique name, so while I have specific privacy settings on my Facebook, I could probably be found just with my name." Furthermore, participants indicated awareness of factors that made searching more difficult: "Only use site-specific photos, din't [*sic*] use the same pictures anywhere else online" (P25, M, 33). "My last name is a common word, so that makes things hard. There's a c-list celebrity with my name" (P32, interview).

Acceptability and etiquette. Some people did not think it appropriate to look people up or thought only certain techniques were acceptable for looking someone up: "I try not

to do anything like that unless I'm planning to meet someone, and even then I'm probably restricting myself to google" (P62, M, 22). 72 thought it was common or very common to look people up. 14 never looked someone up — four said it was an invasion of privacy, the others cited reasons, such as not caring enough to bother. For example, P50: "I honestly never thought about doing this ... I haven't tried any of that - I take dating profiles at face value. Am I supposed to creep on folks?" On the other hand, P11 did not think it took much effort: "I'm really good at using Google to find information about people, so I assume others are too." And some people thought it was common to put in the effort: "Based off of what my friends do, I kind of expect people to really go in and try to figure things out. They're kind of like spies" (P70, F, 24).

Several participants expressed a desire to be covert if they did look someone up: "I won't friend them, but I will scroll through their photos" (P40). Mirroring this, some expressed a preference that others not make it obvious or mention it if they know more than they should. In some cases, users may unwittingly reveal that they have looked up a potential match. For example, P54 (M, 26) was suspicious that someone had looked him up because she appeared in his list of "suggested friends" on Facebook — another example of how the use of multiple apps can affect a user's overall online dating privacy. Other people are okay with or prefer for the person knowing when they find information about them. For example, P31 was unconcerned about the fact that LinkedIn shows who has viewed her profile: she wanted her match to know that she had viewed his profile and for him to look at hers. The timing of disclosing this may be an important factor: "At some point, not on the first date ... but at some point, I prefer to acknowledge the fact that we both looked each other up. Often it happens when you tell them your last name [because they admit they already knew it]" (P56, interview).

2.9 Screenshots

Taking screenshots of online dating content may violate privacy by saving data that might otherwise be ephemeral and taking that information outside of the service, sometimes in

insecure or public ways. 48 participants never took screenshots; two did it once per day or more; and the remaining respondents took screenshots periodically.

Reasons to take screenshots. This study surfaced motivations to take screenshots, including: safety, "just because" (P35, M, 27, interview), to shame rude or inappropriate behavior, to tease users, to avoid registering a profile view (*e.g.,* at odd hours, like the middle of the night (P87, interview)), or for sentimental reasons ("Who wouldn't save their love letters?" (P43, F, 38)). 26 survey respondents took screenshots of especially funny, weird, offensive, or strange content. Respondents also screenshot cute dogs, interesting world views, attractive people, or people they knew.

28 survey respondents shared screenshots with friends (*e.g.,* to get opinions about a potential match or for safety so that someone else had information about the person they were meeting). In addition to sharing with friends, participants reported that they or someone they knew had posted screenshots on social media, *e.g.,* in private Facebook groups or on public forums like a subreddit called "creepypms." Respondents mentioned seeing online dating screenshots that "went viral" on Buzzfeed or other popular news sites. In Section 2.11 I consider how designers might accommodate these motivations alongside users' privacy goals.

Acceptability and etiquette. Some participants viewed screenshots as privacy violations: "I would see it as a huge breach of privacy. Online dating is about putting yourself out there, yes, but screenshotting a dating app conversation is like bringing a tape recorder on a first date. It's just creepy!" (P40). 31 participants said they were not concerned about screenshots because their profiles did not contain sensitive information. Two people said they were not worried because they did not expect to be targeted: "My profile and photos are not then [*sic*] kind of pics [*sic*] that you would fee [*sic*] the need to screenshot" (P40). 14 saw profile content as public information: "Everything is public, it wouldn't bother me" (P73).

A troublesome idea for some participants was the public sharing of screenshots. P81 (F, 27) wrote, "I guess I would be embarrassed if I knew about it (like if it went viral or ended up on Buzzfeed) but I don't care as long as I don't know." Although not asked directly,

three survey respondents thought it inappropriate for screenshots to be used for making fun of people: "It bothers me that someone who is putting themself out there gets teased" (P26, F, 24). Some participants were supportive of or had themselves taken screenshots to publicly acknowledge and condemn inappropriate online dating behavior, although one survey respondent noted: "Sometimes I send rude responses to rude messages, and I wouldn't want those to be screenshotted and spread" (P17, F, 25). A question explored in some interviews was whether screenshots should be de-identified (*e.g.,* faces blurred). P56 felt he was not in a position to judge but thought his friends who shared screenshots on social media *did* obscure faces.

Some people considered messages more private than profiles and, thus, a more serious violation to screenshot: "Honestly I never thought about the messages I sent when I was on a dating site being shared outside of it. If I had I would have been more careful about what I said!" (P18, F, 31). Another participant sent sensitive information in messages: "I hope people don't take screenshots of sexually explicit conversations" (P51, F, 48).

P36 (F, 26) noted users' lack of control over what is done with screenshots, *e.g.,* using Photoshop to alter screenshots: "I think I wouldn't care unless they misuse it by using photoshop to edit it or post it elsewhere which is inappropriate."

2.10 Tinder Profile Analysis

This analysis of Tinder profiles provides ground-truth evidence to support and contrast surveys and interviews. In addition to (1) whether I found the user, I recorded: (2) if photos were reused, (3) if job and/or school were listed, (4) if Instagram was linked or other usernames were listed, and (5) how unique their first name was. In this section, I report the two tailed p-values for N-1 Two Proportion tests.

In total, I found ("found" as defined in Section 2.4) people from 188 of 400 profiles (47%). I saw no significant differences in findability between men and women ($p = 0.11$) or between users in Seattle vs. Atlanta ($p = 0.69$). Of the 188 profiles I found, 75 reused photos from their online dating profile in other places (40%).

Users with linked accounts. Having an explicit link to another account or explicitly listing a username for another service could indicate that a user prefers to be findable. Indeed, the 129 people whose profiles included a linked Instagram account or another username were statistically more likely to be findable ($p < 0.001$) — 103 were findable on other sites (80%). Of the remaining 26 that were not findable, several were "almost findable." That is, I: found them on other services but did not find their full name; found their full name but no other information; or were not confident enough that I found the same person.

However, there are indications that some of these 106 people might not realize they were findable or what other information could be found. Although some had private Instagram accounts, their names and profile photos on Instagram were public. Additionally, I saw at least 11 variations of external services that performed analytics or backups of Instagram — possibly without users' awareness. In some cases, these backups contained information no longer available on Instagram (*e.g.,* full names), speaking again to the challenges of maintaining privacy in a multi-application ecosystem.

Users without linked accounts. Of the remaining profiles, only 85 of 271 were findable (31%). I use this subset of profiles to explore how other information — job, school, and first name — influence findability.

Employment and educational history are imported by default, so users without this information have explicitly removed it or chosen not to include it on Facebook either. Only one of 60 users who did not list a job or school was found. 28 of 106 (26%) who listed either a job or school (but not both) were found. 56 of 104 (54%) who included both job and school were found. Thus, there is a statistical difference in the percentage of people found between those who list neither and those who list one ($p < 0.001$), and between those who list one and those who list both ($p < 0.001$).

The final factor I considered in terms of its impact on findability was a user's name. For people with common names (*i.e.,* >100,000 people in the U.S. share this name according to howmanyofme.com), only 37 out of 140 were findable (26%). For people with less common names, 48 out of 82 were findable (59%). People with less common names were statistically

more findable ($p < 0.001$) — an observation made informally in surveys (Section 2.8).

Observations. Notable content observed in some profiles but not methodically recorded included plans to travel alone, that the person was a recovering alcoholic, references to drug or excessive alcohol use, and other sensitive information. In some cases, users shared content that could make them more findable, including photos of an ID or name tag and recognizable features in the background of photos (*e.g.,* landmarks on college campuses). Distinguishing features, such as unique hair color, made users more recognizable on other sites; in contrast, major changes in appearance could be misleading. Other characteristics that may influence findability but that I chose not to record included content or number of photos, content or length of profile text, indications that someone was using Tinder Plus, and whether a specific job was listed or just the type of work. I also note that people who listed certain jobs (*e.g.,* the specific coffee shop where they worked) may be findable in real life even if they were not findable online.

For some profiles, I found information about users across several sites even if I did not find their full names; for example, some people used the same pseudonyms on multiple sites. Given that some users change their names on Facebook (*e.g.,* to be less identifiable to employers [15]), two tensions arise: choosing a unique pseudonym may make a user *more* findable, and some users may have chosen a pseudonym that does not make the desired impression on potential matches. I also encountered a profile that supported an assertion by P32 (Section 2.8) that having the same name as a celebrity decreased findability.

2.11 Suggestions for Design

A core contribution from this data is to help educate dating site designers so that they can make informed decisions based on users' values and needs, beyond the specific suggestions I make here. I discuss some design implications in the preceding sections; below, I elaborate on two concrete examples of how these findings could inform design.

A key risk of screenshots is content being shared outside of a service, where that service has no control over when and where the content is re-shared. Online dating systems could

introduce features that allow users to achieve their sharing goals while discouraging (or even preventing) screenshots. To provide users agency in protecting their safety, which some currently do by taking screenshots before a date and sharing them with friends, and also to support users' social goals of getting friends' opinions (*e.g.,* of whether a potential match is attractive or how to respond to a message), online dating services could have a built-in feature to (temporarily) share message and profile content and converse with friends directly in the app. To discourage users from mass-screenshotting profiles (as in the Rio example or on Buzzfeed) without preventing practices such as shaming exceptionally offensive behavior, online dating services could restrict the number of screenshots a user may take per day or notify the other party when a screenshot occurs.

There may also be opportunities for new mechanisms to help users control information disclosure. Tinder users might prefer default settings that do not import their employment or educational history, since that information may make them searchable. Tinder could additionally allow users to review and curate their profile before it is visible to others. Tinder Plus users can search for users anywhere in the world, thereby creating a privacy imbalance between the remote and local users. To mitigate this imbalance, Tinder could allow free (or paid) users to disallow remote matches. In addition to addressing privacy concerns raised in this study, this capability might have minimized harms in Rio [19].

Different users have different privacy sensitivities and practices. These results also speak to the benefits of privacy awareness campaigns, whether enacted by industry or a public service organization. Users who are aware of how others might violate their privacy preferences can make better-informed decisions to protect their own privacy. Users who are aware of others' preferences might be more thoughtful when taking actions that could violate privacy preferences.

2.12 Conclusion

This work provides an in-depth study focused on understanding and surfacing users' privacy preferences and practices in online dating. This portrait of the privacy-related aspects of the

online dating ecosystem is the first contribution. Other contributions are the identification of privacy-related tensions and challenges in online dating — challenges that pit privacy directly in tension with other user goals — and specific recommendations for mitigating several key challenges. I hope this work helps inform and focus industry and research efforts on addressing these challenges, thereby helping empower online dating users to more effectively control their privacy while also achieving their other online dating goals.

Chapter 3

A DEEP-DIVE INTO A SPECIFIC INFORMATION LEAKAGE CHANNEL IN USER-TO-USER PRIVACY: ONLINE STATUS INDICATORS ACROSS DIFFERENT APPLICATION CLASSES

In this chapter, I take a focused look at one particular design feature that exists in many popular apps, including several online dating apps — Online Status Indicators (OSIs). Through this work, we can understand how a specific information leakage channel, which is not necessarily relevant to users' goals for using a particular app, can impact their experiences of U2U Privacy. In this work, I explore how subtle differences in the design or implementation of a feature can impact the ways that users interact with apps and with each other. I found that users are aware of what these features might imply about their own or others' real-world behaviors or intentions and that current designs of OSIs lead to app-dependent behavior in which users adapt their behavior to match their desired self-presentation in light of the constraints of an app. The work in this chapter represents a collaborative effort with Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker.

3.1 Introduction

As users move through online spaces and interact with Internet-connected technologies, they leave a vast array of digital traces in their wake. Some traces are left intentionally and are highly visible to the user and to others. For example, users who choose to post on a friend's Facebook page anticipate that their posts will be seen by friends and others. Other traces are left passively, potentially without users' awareness. Companies providing online services keep some of this information about individual users internal within the company (*e.g.*, information gained from cookies that may be used for targeted advertising). However,

some passive digital traces are shared with a wider audience. For example, popular chat apps like WhatsApp expose the time at which a recipient views a sender's message using "read receipts" [67].

Unlike intentionally and consciously shared information — such as posts, profile updates, or messages — passively broadcast records of users' behaviors create an outward presentation of self that users cannot easily control, even when they know the records are being generated. This can expose users to unknown, unavoidable, or unpredictable risks. Developing a more robust understanding of the impact of passive digital traces on users and their potential for adversarial use will help the research community better advocate for consumers.

Here, I examine the passive digital traces left by Online Status Indicators (OSIs). OSIs are UI elements that automatically broadcast when a user comes online or goes offline. They signal to users when others are potentially available for conversation, multiplayer gaming, or various social interactions; if the user is offline, they indicate that it might not be a good time to send a message or that the recipient is unlikely to respond quickly.

While these uses of OSIs can improve users' experience, prior work has found that OSIs can leak sensitive information [37], such as sleep-wake routines, workplace distraction, conversational partners, and deviations from daily schedules. Although this finding is troubling, we currently lack a robust understanding of how and when OSIs project sensitive information, how aware users are of the passive traces they leave, or what users think about these designs.

- The first contribution of this work is an *analysis of the OSI design ecosystem.* I systematically chose 184 mobile apps for analysis in order to characterize OSI designs. Across apps, I found that OSI design varies substantially in terms of visual appearance, audience, reflection of user behavior, and implementation of OSI-related app settings. Using this input, I then sought to understand how users cope with the surprising, if sometimes subtle, variations in OSI implementations.

- The second contribution of this work is an online survey of users' knowledge about

and reactions to OSIs, which I deployed to 200 workers on Mechanical Turk. I found that although participants could generally recognize an OSI, they held many uncertain or incorrect beliefs about their functionality. They were often mindful of information their own OSIs might convey to others, and many reported altering their own behavior as a result. I found that participants both notice and make inferences based on other people's online status, sometimes reacting to it in potentially problematic ways (*e.g.*, surveilling intimate partners). Drawing on existing constructs of *app enablement* and *app dependence* [59], I show how current OSI designs lead to app dependence (*i.e.*, behaviors dictated by the app rather than the user's intrinsic needs and desires) and prompt users to contort their behaviors to manage their OSI display.

- The third contribution is a set of *concrete design recommendations for app designers.* Using the empirical data from both the app analysis and user survey, I present guidance for creating OSIs that are consistent with users' mental models and considerate of user preferences.

3.2 Related Work

This research builds on and contributes to a broad body of work related to digital traces, messaging apps, and user experiences with privacy settings. A *digital trace* is data that reveals information about the activities a person engages in online. It includes both the content a user posts intentionally and additional meta-information that is recorded as a byproduct of user behavior. We all leave digital traces as we interact with computers and other digital devices, ranging from smartphones to fitbits [20].

According to Goffman, people seek to manage in-person impressions based on context and audience [61]. Likewise, users' preferences about managing online impressions are influenced by a variety of factors, including what information is being shared, at what granularity, and with whom [32, 33, 69, 73, 42, 103, 110]. Since digital traces include OSIs that are broadcast to others, they represent an outward presentation of self that users may seek to curate

or control. Although they may develop strategies and techniques to do this [108, 79, 80], many obstacles interfere with their success. This chapter describes obstacles to managing impressions based on OSIs.

In addition to the raw data itself that is left as a digital trace, other information may be inferred, or "leaked," from the raw data that is more amenable to adversarial use. For example, several studies found that the content users post on social media correlates with whether they have health conditions such as depression and addiction [95, 98, 46, 105]. Records of the use of specific devices or apps (*e.g.,* what apps someone are used, for how long, and patterns of usage) can be used to infer information about users' real-world and online activity [31, 35, 52, 37].

Buchenscheit et al. monitored online status of groups of friends on WhatsApp and found that online status can reveal what time people awaken or go to bed, their typical schedule, whether they deviate from that schedule, if they are using apps while at work, and, in some cases, which people within a group are conversing privately [37]. Although they found that participants were not excessively concerned about their own privacy, some participants discussed using OSIs to actively monitor or make inferences about their friends, and the authors discuss potential contexts in which information leaked via OSIs could be highly sensitive, for example, when used for surveillance in relationships with power imbalances (*e.g.*, abusive romantic relationships) or by employers to monitor and predict employees' work performance.

Do et al. found that the app(s) someone is using are predictive of a person's physical location, and vice versa [52]. Authors such as Böhmer et al. have further studied these and other patterns of app use and proposed leveraging them to create tools that suggest to users the app that they are most likely to want to use [35]; however, wide-scale deployment of such tools in conjunction with existing OSIs could exacerbate a hypothetical adversary's ability to make the inverse inference of where someone is located based on the app they are using.

Many features beyond OSIs may reveal when someone is (or was) online and, thus, act as imperfect proxies for OSIs, *e.g.*, time-stamps on posted content. Many popular messag-

ing apps, including WhatsApp, iMessage, and Facebook Messenger, have "read receipts" in addition to or instead of OSIs to inform message senders whether recipients have read the message. Even if users were able to configure privacy settings for OSIs, other sources of presence information may have separate or non-existent privacy settings. Privacy considerations and user experiences related to read receipts have been addressed in research and in the media [12, 26, 6, 67].

In addition to the work by Buchenscheit et al., a paper from 2000 studied 20 people's use of Instant Messenger (IM) at work [89]. It identified "awareness information about the presence of others" as a key IM feature (*i.e.*, an early implementation of OSIs that indicated when someone was logged into a service like AOL Instant Messenger (AIM)). Although participants discussed observing patterns in their coworkers' online status that correlate with real-world behaviors even when they were not planning to contact those people, this work did not directly address the privacy implications of these observations. They instead focused on the benefits that IM can provide in the workplace; they found that presence information made it easier for users to "negotiate availability" than did email or face-to-face conversations. That is, presence information let users assess whether it was a good time to contact someone but also allowed the recipient to choose a good time to respond. The authors recommended that presence indicators provide *less* "awareness information" to provide message recipients with plausible deniability as to whether they were actually online, which participants cited as a useful characteristic of OSIs in AIM. A broad body of follow-on work explored the possibilities for using "awareness" to improve online conversation and collaboration, for example, by making it peripherally noticeable so that IM conversations were less distracting when users were busy [28, 29, 47].

Relevant concerns have also emerged in work that focused on topics or contexts besides OSIs. For example, Hancock *et al.* studied lies people tell online, in particular "butler lies" that are frequently used to gracefully exit a conversation (*e.g.*, "sorry, I've got to go to sleep now.") [64]. They hypothesized that since users typically tell butler lies at the end of conversations, they might have preferred to avoid the conversation altogether; they

recommend that apps allow users to determine whether *specific contacts* are able to see their online status. Freed et al. found that easily accessible information on phones and in apps was leveraged by abusive partners [56, 57, 82]. Though they did not mention abuse of OSIs specifically, victims and survivors of domestic abuse might experience heightened privacy risk due to their partner's observations of their OSIs. In fact, Guberek et al., studying technology and privacy considerations of undocumented immigrants, explicitly mention a participant's concern about her ex-partner keeping track of her via OSIs in WhatsApp [62].

3.3 Methods for App Analysis

The first component of the methodology, app analysis, involved identifying the set of apps to evaluate. I then applied an iterative analysis process inspired by qualitative grounded theory to explore OSI design patterns in the selected apps. This iterative process resulted in a rigorous set of analysis steps for each app, shown in Figure 3.1 and described fully in Section 3.3.3. Analysis occurred from June 4 through September 14, 2018. The scope of OSI observations was limited to smartphone apps. Note that the implementation of OSIs in mobile apps may differ for desktop or browser-based versions of the same app. Additionally, since app companies may at any time be A/B testing their products, exact behaviors or interfaces I observed in an app may not represent what all users would have seen during the study period.

3.3.1 Identifying apps for analysis

My goal was to comprehensively explore OSI design patterns for a select set of apps. I used the following diverse criteria to identify apps, with an intentional bias toward ones that are popular or already known to have OSIs:

- *Top-rated apps by category:* I also included the 5 top-rated free apps in each of 13 categories and the top 10 free apps in the social category on June 4, 2018, as archived on App Annie (for the Google Play Store [23]).

Google Play Store Top Apps by Category (Rank Order within Category)			Google Play Store Top 50 Apps (alphabetical)	Novice Suggestions	Apps Used by Participants in Prior Study	Expert Suggestions
Books & Reference		Food & Drink	Amazon Shopping (3)	**Discord (3)**	**MyFitnessPal**	Airbnb
King James Bible	Events	Uber Eats	Android Auto	Dual!	Chase Mobile	**Battle.net**
Audiobooks from Audible	Ticketmaster	DoorDash	Baseball Boy	Flickr	Dropbox	Bumble
Bible	StubHub	McDonald's	Color Road	Flipkart	eBay	Candy Crush
Amazon Kindle	Gametime	Grubhub (2)	DHgate-Shop	Gmail (3)	Google Calendar	Canvas (student portal)
Libby, by OverDrive	SeatGeek	Domino's Pizza USA	Draw In	**(Google) Hangouts (3)**	Google Drive	CareZone
Communication	Vivid Seats	Medical	Episode -- Choose your story	Google Plus	Google Docs or Google Sheets	Castlight Mobile
(Facebook) Messenger (1,2,3)	Family 5 & Under	MyAir	Flip the Gun	Google Voice (3)	Google Keep	eharmony Dating
WhatsApp Messenger (1, 2, 3)	YouTube Kids	MyChart	Flying Arrow	**Grindr**	Google Opinion Rewards	Facebook Local
(Facebook) Messenger Lite (1)	(also in all other Family categories)	GoodRx	Granny	**Hike**	Google Play Music	Fitbit
Marco Polo Video Walkie Talkie	Toca Kitchen 2 (also in Family 6-8)	FollowMyHealth	Helix Jump	**imo**	Imgur	Glow Baby
Yahoo Mail	PBS Kids Games	Ada	**Jurassic World Alive**	Kik	Lookout Security & Antivirus	Goodreads
Dating	PJ Masks: Moonlight Heroes	Music & Audio	Kick the Buddy	Line	Lyft	GroupMe
Zoosk Dating	Family 6-8	Pandora (1, 3)	LetGo	**LinkedIn**	(Google) Maps	**Happn**
Match Dating	**(Facebook) Messenger Kids**	Spotify (1, 2, 3)	Love Balls	Mindmeister	Nova Launcher	**Hearthstone**
CoffeeMeetsBagel Dating	**(also in Family, overall)**	Free Music Plus (1)	News Break: Local	MyRadar	OneBusAway	Hinge Dating
OkCupid Dating (2)	LEGO NINJAGO: Ride Ninja	SoundCloud	**OfferUP**	Reddit	reddit is fun (unofficial)	iHeartRadio
JOYRIDE Dating	Chuck E.'s Skate Universe	YouTube Music	Partymasters	Signal	Robinhood	Indeed
Education	Family, overall	Social (Top 10)	Pixel Art: Color by Number Game	**Skype**	Slack	Insight Timer
Duolingo	**ROBLOX (1)**	Snapchat (1, 2, 3)	**PUBG MOBILE**	Surfline	Starbucks	Memrise
ABCmouse.com (also in Family 5 & Under)	No.Draw	**Instagram (1, 2, 3)**	Rise up	**Telegram**	Swagbucks	Nextdoor
Language Translator: easy, free, efficient	No. Color	**Facebook (1, 2, 3)**	Run Sausage Run	Tinder (3)	T-Mobile Tuesdays	**Steam**
Lumosity	Finance	musical.ly (1, 2)	Sling Drift	Topbuzz	Textra SMS	Strava
Remind: School Communication	Cash App (1)	TextNow (1)	slither.io	**Tumblr (3)**	**Waze**	Whisper
Entertainment	PayPal (3)	FindNow	Snake VS Block	**Twitch**	Yelp	**Words with Friends**
Netflix (1,3)	Venmo(3)	Messages, Text and Video Chat for Messenger (NOT Facebook)	Subway Surfers	Twitter (3)		Yousician
Bitmoji (1)	CreditKarma		The Cube	UC Browser		**Yubo**
Google Play Games (1)	Bank of America	Pinterest (2, 3)	Toon Blast	**Viber**		
Hulu (1)		**Facebook Lite**	Uber (3)	WeChat		
Amazon Prime Video (1)		**POF (Plenty of Fish) Dating**	Will it Crush?	YouTube (3)		
			Wish			
			Word Link			

grey text - no social features
normal black text - has social features (but not OSIs)
bold - has typical online status indicators
Underline - has sub-area online status
blue - (typical) online status can be turned off
red - (typical) online status cannot be turned off
(1) App is also in Top 50 Apps
(2) App is also in Novice Suggestions
(3)App is also in real app usage data

Table 3.1: The 184 apps included in analysis, sorted by inclusion criteria. Numbers next to apps indicate that they fall within multiple inclusion criteria. Apps are demarcated with font color and style based on high-level findings, such as whether the app has social features or OSIs.

Figure 3.1: Workflow for systematically analyzing OSI design patterns in each app.

- *Top-rated apps in general:* From the Google Play Store, I included the top 50 free apps on June 4, 2018, as archived on App Annie [22].

- *Novice users' app suggestions:* I showed 50 novice users on Mechanical Turk a screenshot of OSIs from the browser version of Facebook and asked them to name 3 apps or services "that you know or believe have online status indicators" and 5 apps or services "that you think might have online status indicators." I included 40 apps suggested by these users that I could find in the Google Play Store.

- *App usage patterns:* I contacted the authors of a prior work [76], who shared data from 45 participants' phone usage behaviors, including which apps participants had used during a two-week period. I included the 48 apps used by at least 10% of participants.

- *Expert users' app suggestions:* Finally, I included 27 additional apps based on recommendations from expert users, including myself and my collaborators. For example, our expertise was informed by conversations with teenagers at a University-sponsored CS outreach event that was not part of this study, who told us about the app Yubo.

In total, I identified 184 apps for analysis, shown in Table 3.1.

3.3.2 Initial Analysis and Reliability Coding

Initial questions I used for first-round coding were: (*Q1*) Does this app have any social features?, (*Q2*) Does this app have OSIs?, and (*Q3*) If the app has OSIs, can they be turned off? The researcher took notes of additional observations. Although all 184 apps were free to download, some apps required a paid account or special credentials to use. To explore OSIs despite this limitation, the researcher based the analysis on information available in the Google Play Store or from online searches for 16 apps. For 13 apps, the researcher used a personal account and/or device (iPhone) for analysis. For example, Steam allows users to connect as friends only after they have both spent $5 in the app; therefore, instead of

spending $5 on multiple research accounts, the researcher used a personal account and help from a friend with a Steam account to understand OSIs in this app.

A second coder independently analyzed *Q1*, *Q2*, and *Q3* for 32 apps chosen by the primary coder (*i.e.,* 9 apps with varied implementations of OSIs and 23 apps without OSIs). For those with OSIs, the second coder additionally recorded the default audience and settings for OSIs (if applicable) and took open notes about other OSI details. Reliability provided confidence that there were no false negatives regarding the existence of OSIs in apps (*Q2*). Researchers were in agreement except for one app that only the primary coder identified as having OSIs. Reliability coding also served to ensure that there were no false negatives regarding the ability to change app settings for OSIs (*Q3*). Excluding the one app noted above, coders found the same results for this question. Coders disagreed about whether 4 apps had social features (*Q1*); although this was not the study's main focus, disagreement was resolved by refining our working definition of "social features" as being between two user accounts (*e.g.,* excluding Hulu and Netflix, where multiple users log in with the same credentials), excluding users with special permissions or privileges (*e.g.,* ABCMouse.com, an educational app, lets parents monitor their childrens' progress, but I do not consider this a social feature since parents have special privileges within the app); and excluding features that let users send "invite codes" or share updates outside of the app (*e.g.,* via a link).

3.3.3 Final App Analysis

Through a discussion guided by both coders' open notes, the research team generated specific themes related to the scope, audience, settings, appearance, and how long it takes before users appear as online/offline after opening/closing an app. I conducted a final round of analysis based on these themes using two factory-reset phones with fresh SIM cards and the following systematic analysis protocol:

1. Create Facebook accounts on both phones but do not connect them as friends. For some apps, users can access substantial amounts of functionality without creating accounts.

For example, many Waze users may not realize that it is even possible to create an account because their main reasons for app usage (*i.e.,* getting directions) can be accomplished without doing so. My OSI observations are made assuming that users *have* created accounts, and I do not classify the extent to which each app could be used without one. This caveat is be most relevant in terms of how it impacts my discussion of participants' knowledge of the existence of and default audience/settings for OSIs in the Mechanical Turk survey (Section 3.6.3).

2. Observe default settings on all Facebook apps (Facebook, Messenger, Facebook Lite, Messenger Lite, Messenger Kids).

3. Conduct app analysis for other apps using the canonical workflow for analyzing a single "typical" app illustrated in Figure 3.1, signing in through Facebook only when needed.

4. Finish app analysis for Facebook apps.

5. For some apps, I could not connect accounts as friends without their being Facebook friends. In this case, I observed default settings in those apps at step (3) and then finished analyzing them as the final step.

This protocol was designed to account for ordering effects observed in initial app analysis. For example, I wanted to observe how (or if) an OSI appears to an unconnected user in each app. Because friends are consistent across Facebook apps and some apps automatically sync friends from Facebook if users sign into that through Facebook, it was important for these apps to be analyzed *before* connecting the accounts as friends on Facebook. Using new phones and accounts and this systematic process let me carefully observe default app settings that I had not previously recorded. Additionally, some aspects of OSIs must be observed at a specific phase in the connection of users (*e.g.,* if OSIs are visible to either user once a friend request or initial message has been sent but before it has been accepted or reciprocated).

To account for natural variance in measurement of time to come online or go offline (Action 10 in Figure 3.1), I measured timing information while phones were on the same wifi network, and I report timing in coarse-grained buckets. There is substantial nuance to *how* I measured the time for users to appear as online or offline. Taking an adversarial mindset, I aimed to measure the approximate granularity with which a focused but not technically savvy adversary could track another user's online status. Thus, the "shortest time" measurement in Figure 3.1 denotes that if the adversary can *reliably* reduce the time it takes to see an updated OSI by repeatedly refreshing the page or closing and reopening the app, I *do* perform those actions. For most apps, I conducted 5 to 10 timing measurements while varying how the observed user exited the app (*e.g.,* turning off the phone, going back to the home screen, "hard quitting the app," or opening a different app); however, I collected fewer and less precise measurements for apps with a time-to-offline that exceeded one hour. I did not collect timing measurements for apps where I could not view other research account profiles (*i.e.,* in dating apps, where users are randomly shown profiles of other users, and on OfferUp) or for MyFitnessPal because it took too long for users to appear as offline.

3.4 Taxonomy of Online Status Indicators

I now describe the design space of OSIs and the prevalence of common design patterns, referring frequently to examples from apps I analyzed. All screenshots were edited or reproduced to replace identifying information from real users with generic profile photos and generic user information.

Of the 184 apps analyzed, 116 had social features (defined in Section 3.3 and shown in black, red, or blue in Table 3.1). Forty of the 116 apps with social features had OSIs (bold and/or underlined in Table 3.1). The analysis in this section is informed by the OSI design patterns in these 40 apps.

I start with a revised definition and discussion of terminology. I next cover: appearance of online users, appearance of offline users, audience, settings, and connection to ground-truth user behaviors. Table 3.2 shows a simplified summary of common design patterns in each of

these categories for all apps.

3.4.1 Terminology

Prior work and language within existing apps uses a variety of terms, such as "online status," "active/activity status," "presence," "availability," or "last seen," to describe what I refer to as an OSI; some apps do not give an explicit name to the feature at all. Here, we precisely define the term as being OSI any feature that: (1) is intended to reveal to a user whether another user is or was recently online (*i.e.,* accessing an app, service, or specific space/content within the app), and (2) passively updates as users come online and go offline. OSIs across apps reflect users' behavior with a wide range of accuracy and precision, but this does not affect whether I have included these OSIs in my analysis.

For the remainder of this chapter, I refer to *online status* and *online status indicators (OSIs)*. I use these terms in subtly different ways. An OSI refers to a visual element that indicates whether someone is online. Online status is the value that this indicator has or the information that the indicator conveys (online or offline), which may or may not match the user's current behavior. For instance, it may take a measurable amount of time for an app to reflect that someone has stopped using it, in which case the person's OSI might show the user's status as online although they are not. In some apps, users can permanently set their online status to offline but continue to use the app. In this case, their online status is offline even when they are actually online. When the user's actual behavior is important, I use longer phrases, such as "whether the user is online" or "that the user is active."

In apps that include configurable settings for OSIs, I generally refer to the OSI as being "on" or "off" depending on whether the app displays the icon and updates its appearance to reflect the user's online status. Where necessary, I use additional verbiage to specify more nuanced information about how an OSI looks or functions when it is "off." This is particularly relevant in Section 3.4.6 where I describe the apps for which an adversary could detect whether someone has turned off their OSI or is *actually* offline.

	AUDIENCE				SETTINGS	APPEARANCE			TIMING	
App	TYPE(S) OF OSI (SCOPE)	(DEFAULT) RELATIONSHIP WITH USERS WHO CAN SEE OSI	CAN (OR MUST) SIGN UP WITH OTHER SERVICE	APP HAS OSI SETTINGS	GREEN DOT FOR "ONLINE"	APPROXIMATE OR EXACT LAST ONLINE TIME	CLICKS TO SEE AN ONLINE STATUS	VISIBILITY OF SELF	TIME TO ONLINE	TIME TO OFFLINE
	Typical, Sub-area, or Cross-app	● (Friends/connections), ○ (Global), or Other	Yes or No	Yes or No	● (Yes) ◢ (Yes, but with caveats)	Approximate or Exact	0 to 3 or Other	Yes or No	• (A few seconds), ● (A few minutes), -- (Not measured), or Other	
Battle.net	Cross-app (w/ Hearthstone)	●	Yes	Yes	●	Approximate	0	Yes	•	several hours
Canvas (student portal)	Sub-area	Anyone w/ access to group chat (restricted)	No	No	●		3	Yes	•	•
Coffee Meets Bagel Dating	Typical	○	Yes	No		Approximate	must pay	No	--	--
Discord	Typical	●	No	Yes	●		0	Yes	•	●
Facebook	Cross-app (FB Grouping)	●	No	Yes	●		0	No	•	●
Facebook Lite	Cross-app (FB Grouping)	●	No	Yes	●		0	No	•	10-60 minutes
Google Docs or Google Sheets	Sub-area	Anyone w/ access to doc or sheet	Yes	No			1	No	•	•
(Google) Hangouts	Typical	●	No	Yes	◢	Approximate	1	No	•	10-60 minutes
	Sub-area	Other person in conversation		No			0 once in sub-area	No	•	•
Grindr	Typical	○	No	No	●	Approximate	0	Yes	•	10-60 minutes
Happn	Typical	○	Yes	No		Approximate	1	No	--	--
Hearthstone	Cross-app (w/ Battle.net)	●	Yes	Yes (only via Battle.net app)		Approximate	1	No	•	several hours
Hike	Typical	●	No	Yes		Exact	1	No	•	•
imo	Typical	●	No	Yes	◢	Exact	1	No	•	●
	Sub-area	Other person in conversation		No			0 once in sub-area	No	•	•
Instagram	Typical	●	Yes	Yes	●		1	No	•	●
JOYRIDE Dating	Typical	○	Yes	No	●	Approximate	0	Yes	--	--
Jurassic World Alive	Typical	Not observed	Yes	No	◢		1	No	•	●
LinkedIn	Typical	No one, but app automatically changes to ● after some use	Yes	Yes	●		2	Yes	•	●
Marco Polo Video Walkie Talkie	Typical	○	No	No		Approximate	2	No	•	●
Match Dating	Typical	○	Yes	No	●	Approximate	0	No	--	--
(Facebook) Messenger	Cross-app (FB Grouping)	●	Yes	Yes	●	Approximate	0	Yes	•	●
(Facebook) Messenger Kids	Typical	●	Yes	No	●		0	No	●	●
(Facebook) Messenger Lite	Cross-app (FB Grouping)	●	Yes	Yes	●	Approximate	0	Yes	•	●
MyFitnessPal	Typical	●	Yes	No		Approximate	2	Yes	--	--
OfferUP	Typical	○	Yes	No		Approximate	2	No	--	--
OkCupid Dating	Typical	○	Yes	No	●		0	No	•	10-60 minutes
Plenty of Fish (POF) Dating	Typical	○	No	No			1	No	--	--
PUBG MOBILE	Typical	●	Yes	No		Approximate	1	No	•	●
ROBLOX	Typical	●	No	No	◢		2	Yes	•	10-60 minutes
	Sub-area	Anyone w/ access to mini-game (most are public)		No			1 once in sub-area	Yes	•	•
Skype	Typical	●	Yes	Yes	●	Approximate	1	Yes	•	●
Slack	Sub-area	Anyone w/ access to workspace (restricted)	Yes	Yes	◢		1	Yes	•	•
Steam	Typical	●	No (& must sign up in browser)	Yes		Approximate	0	No	•	•
Telegram	Typical	●	No	Yes		Exact	0	Yes	•	•
Tumblr	Typical	○	No	Yes	●	Approximate	3	No	●	10-60 minutes
Twitch	Typical	●	No	Yes	●		1	No	•	10-60 minutes
Viber	Typical	○	No	Yes		Approximate	1	No	●	●
Waze	Typical	●	No	Yes		Approximate	3	No	●	●
WhatsApp Messenger	Typical	○	No	"Last Seen" Settings		Exact	2	No	•	•
Words with Friends (classic)	Typical	○	Yes	No	●	Approximate	0	No	●	10-60 minutes
Yubo	Typical	●	No	No	●	Exact	1	No	•	•
Zoosk Dating	Typical	○	Yes	No	◢		0	No	--	--

Table 3.2: A simplified description of design patterns in 40 apps with OSIs.

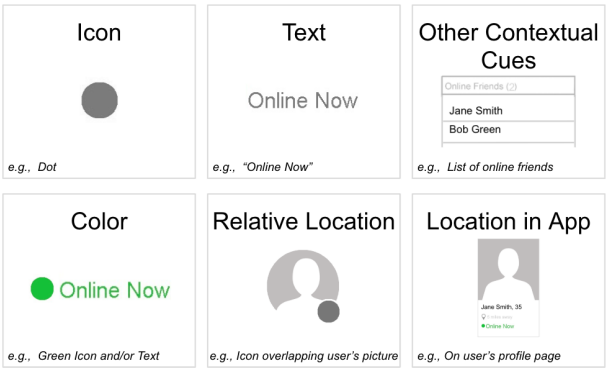


Figure 3.2: OSIs can consist of a subset of several abstract components: an icon, text, and other contextual cues. Each of these abstract components can assume a specific color, relative location, and/or location within the app.

3.4.2 OSI Appearance for Online Users

Below, I describe the most common OSI design patterns when users are online.

Green Dots and Other Icons

Green dots that to indicate a user is online are present in 21 of 40 apps I reviewed. They can be placed close to a user's name or profile picture thumbnail (overlapping it), or elsewhere on a user's profile page.

Variation exists even among green dots. For example, the "imo" app's green dot has a white check mark in it (Figure 3.4). Green dots across apps also use various shades of green, even in apps made by the same company (see Facebook and Messenger in Figure 3.3).

Firugre 3.4 shows additional variations of OSI icons for online users, including other icon shapes and colors. CMB uses a clock-like icon (and text) to indicate whether the user has been online within 72 hours. Jurassic World Alive and ROBLOX use different colored dots to convey that the user has the app open, though both of them use a green dot to show when a user is playing a game and does not *just* have the app open. OSIs for "Single-channel guests" in Slack workspaces use a triangle icon instead of a dot; Slack also lets users choose different

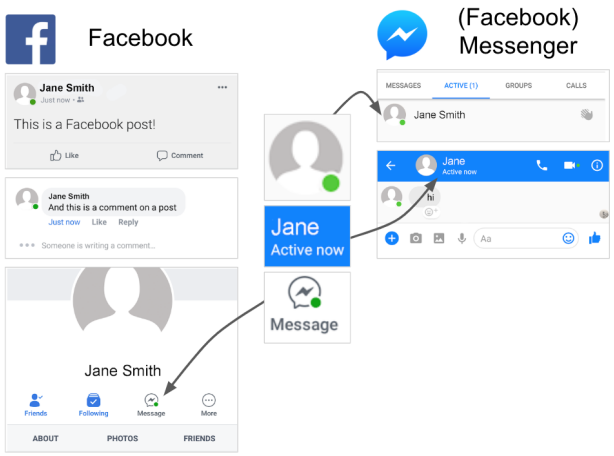


Figure 3.3: In Facebook Apps (*i.e.,* Facebook, Facebook Lite, Messenger, and Messenger Lite), OSIs appear in several locations within the app. Shown here are green dot OSIs in/on a post, comment, user's profile, list of online friends, and conversation view. OSI appearance (*e.g.,* different shades of green) can vary within and across apps.

color "themes," which affects the color of OSIs in the sidebar view (Figure 3.4). Variations in icons used to indicate when someone is online could be misleading to users, particularly for apps that deviate more from the most common colors or shapes.

Text

Several apps' OSIs contain text rather than or in addition to icons. For example, POF Dating does not use an icon for OSI, though the green color of the text associates it with green icons in other apps (Figure 3.4). Text can help disambiguate the information conveyed by an OSI, but it is sometimes used to convey more detailed information about what a user is doing. For example, Hearthstone, Battle.net, ROBLOX, and PUBG Mobile all use text to specify more about what users are doing in the app (*e.g.,* which game they are playing). Hangouts and Battle.net use text to convey whether a user is accessing the app via a mobile device.

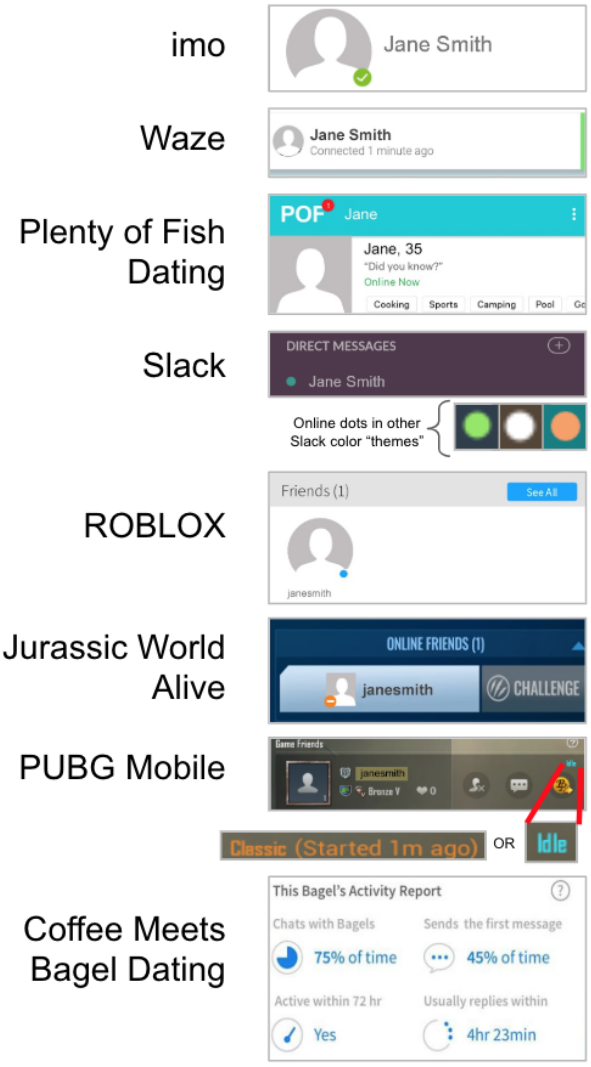


Figure 3.4: Beyond simple green dots, apps use a wide variety of icons and text to show that a user is currently online.

Other Facets of OSI Appearance

Thirteen of 40 apps let users see their own OSIs. For example, in the screenshots of OSI settings in Figure 3.9, Facebook Messenger (c) and Battle.net (g) both show green dots near the active user's profile picture, which change in appearance if users turn off their OSIs. This could be a helpful cue to remind users that their online status is visible to others.

Some apps actively notify users when their friends come online. For example, Facebook Messenger briefly displays a banner that says "[friend's name] is active now." Marco Polo Video Walkie Talkie has a similar feature and, although it does not have online status settings, lets users exclude themselves from these "activity updates." One might question whether these notifications make users more aware of the information they are passively sharing.

3.4.3 OSI Appearance for Offline Users

When users' OSIs change to show that they are offline, any text and/or icons may disappear or change in some way. Figure 3.5 shows examples of offline vs online users' OSIs.

Last Online Time

Twenty-five of 40 apps specify how long ago the user was online through text (Figure 3.6). This creates a more persistent record of activity than OSIs that show only online status. For example, if someone is online in the middle of the night, anyone who comes online before that person's next use of the app could see that they were active at an unusual hour. Of those 25 apps, 5 reveal exactly what time the user was last online, and 15 give an approximation, such as "last seen 4 hours ago." Note that an active adversary or automated tool could still infer more fine-grained information.

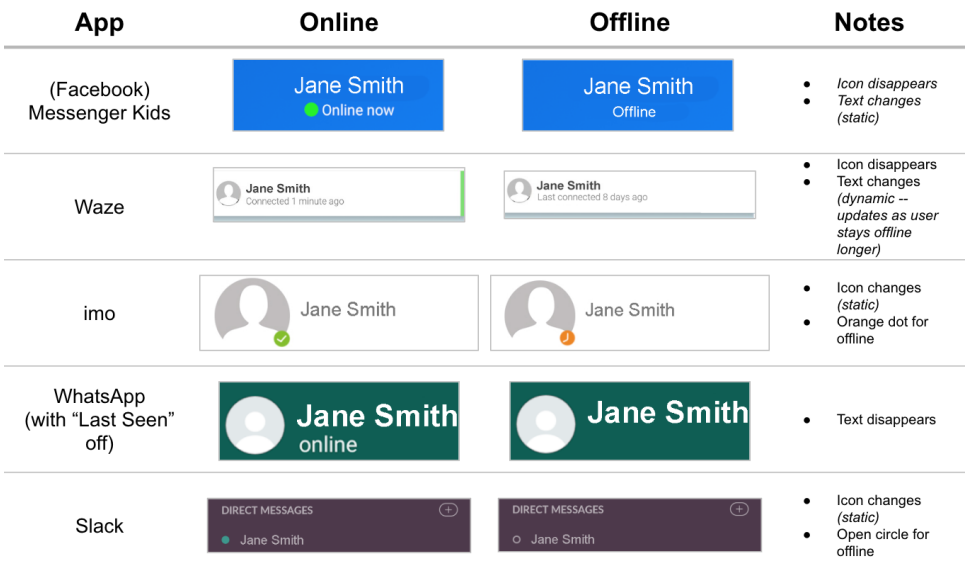


Figure 3.5: Examples of transitions from online to offline. Icons and/or text may go away or change. If the icons or text change, they may do so either statically or dynamically. That is, in some cases, the text or icon may continue to change as the user stays offline for longer, typically to indicate how long the user has been offline.

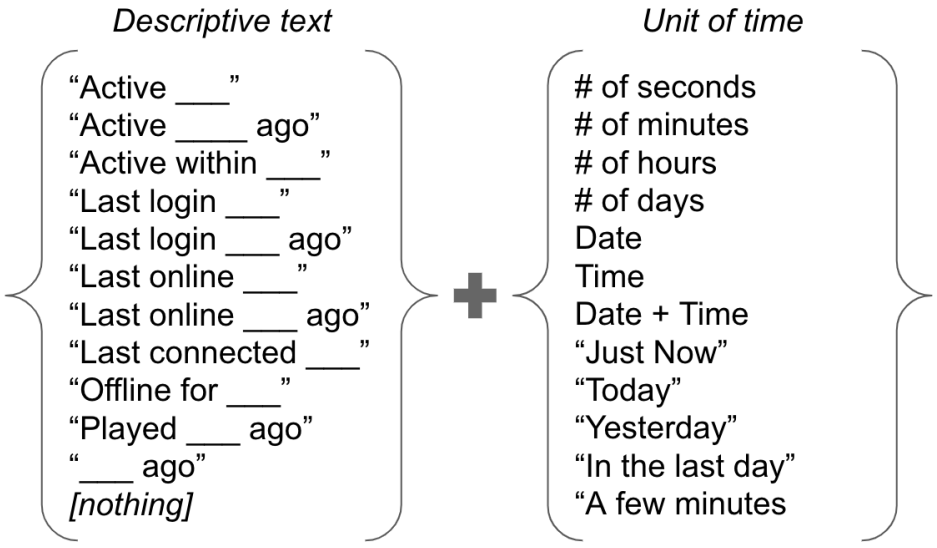


Figure 3.6: Possible text combinations for indicating when a person was last online.

3.4.4 Audience

The default audience for an OSI is determined by: (1) the relationship between users (*e.g.,* whether or not they are "friends" or "contacts" within the app), and (2) the scope of what users are accessing or doing in an app (*e.g.,* "where they are" relative to each other in terms of which part of the app(s) they are accessing).

Relationship to Other Users

The relationship between users — *e.g.,* if users are "connected" as friends, contacts, etc., is one aspect of an OSI's audience. The top right and bottom left images in Figure 3.7 illustrate a typical OSI that is visible to only connections and one that is visible to all other users.

Fourteen apps expose OSIs to *any* other user of the app by default, though it may be nontrivial to find a specific person in these apps. For example, in dating apps like Grindr and Match, profiles (including OSIs) are visible to nearby users, so users will see *someone's* OSI, though it might be difficult to look up *specific* users. On the other hand, WhatsApp users can be looked up from their phone numbers.

Twenty apps have OSIs with default visibility only to connections. Of these, 9 let users sign in or sign up via another service such as Facebook, which could result in friends or connections being automatically synced between apps, making it harder for users to anticipate who can see their OSIs. LinkedIn does not show online status to *anyone* at first; however, audience settings are automatically updated such that OSIs are visible to connections. It was not obvious and beyond my research scope to understand what prompts this change. I draw attention to this feature because it could be especially confusing to users.

Scope in App

Users' "location" within an app relative to other users can factor into the audience of an OSI. The most prevalent scope for an OSI is between users accessing the same app, present in 37 of 40 apps. I refer to this as a *Typical* OSI. Other OSI scopes are *Sub-Area* and *Cross-App*,

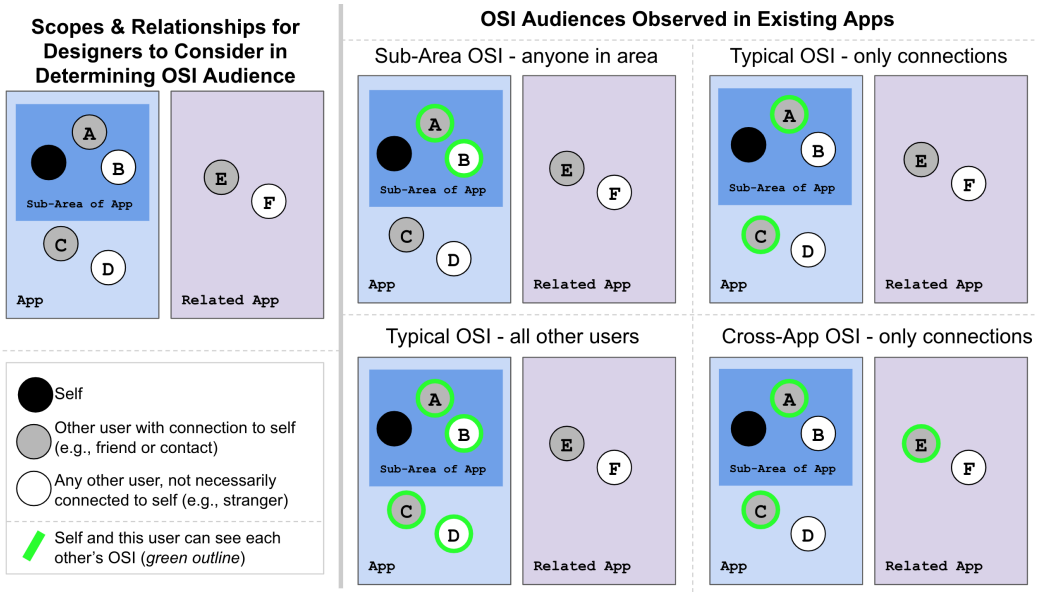


Figure 3.7: OSI designers should consider which other users should be able to see someone else's online status and under what conditions, in terms of: (1) *relationship* — whether users are connected as friends, contacts, etc. and (2) *scope* — "where" in the app the users are relative to each other. OSIs visible to other users "in the same place" (*i.e.*, accessing the same sub-area of an app) may simulate physical proximity in the real world and limits audience in one "dimension;" however, OSIs visible within a sub-area implicitly reveal more about *what* the users are doing rather than just *that* they are online. The four figures on the right show default OSI audiences in existing apps.

illustrated in the top middle and bottom right images in Figure 3.7, respectively.

Sub-Area OSIs implicitly tell users that they are accessing the same sub-area of an app. They will likely not be observable the *whole* time users access an app, but they reveal specific information about what users are doing. Three apps have *only* Sub-Area OSIs: Slack within workspaces, Canvas for discussion boards, and Google Docs or Sheets for shared documents. Three apps have both *Typical* and *Sub-Area* OSIs. Hangouts and imo have conversation-level indicators that reveal when a chat partner is viewing the conversation, shown in Figure 3.8. ROBLOX shows a list of other users playing the same mini-game. The (default) audience for Sub-Area OSIs may differ from the audience for Typical OSIs even within the same app. For example, in ROBLOX, only friends can see Typical OSIs. This Typical OSI also happens to specify which mini-game a friend is playing, but the scope of what the observer is doing (*i.e., not* playing the same mini-game) makes it a Typical rather than Sub-Area OSI. However, anyone else playing the mini-game, which typically has unrestricted access, can see other users playing the same mini-game. In all apps I analyzed, mutual presence in a sub-area was sufficient to describe the audience of a Sub-Area OSI, though some apps restrict access to the sub-area.

Cross-App OSIs have a larger scope than a single app. When users open one app, their OSIs are visible to users in another app. Two sets of apps I studied have Cross-App OSIs: (1) Battle.net and Hearthstone, and (2) Facebook, Messenger, Facebook Lite, and Messenger Lite. I identified these sets of apps from personal use and knowledge of the apps rather than systematic analysis, so it is possible that other apps have Cross-App OSIs that I labelled Typical OSIs. In both of these groups of apps, the same account is used to access all apps. In terms of audience, this means that "friends" or other connections are consistent across apps (*i.e.,* Facebook friends match Messenger contacts). However, this behavior may still surprise users and, as relate in Section 3.4.5, other aspects of Cross-App OSIs may place additional cognitive load on users. In terms of privacy implications, Cross-App OSIs do not necessarily reveal as much as Typical or Sub-Area OSIs about what the observed user is doing, though in practice I observed that the former sometimes specify which app the

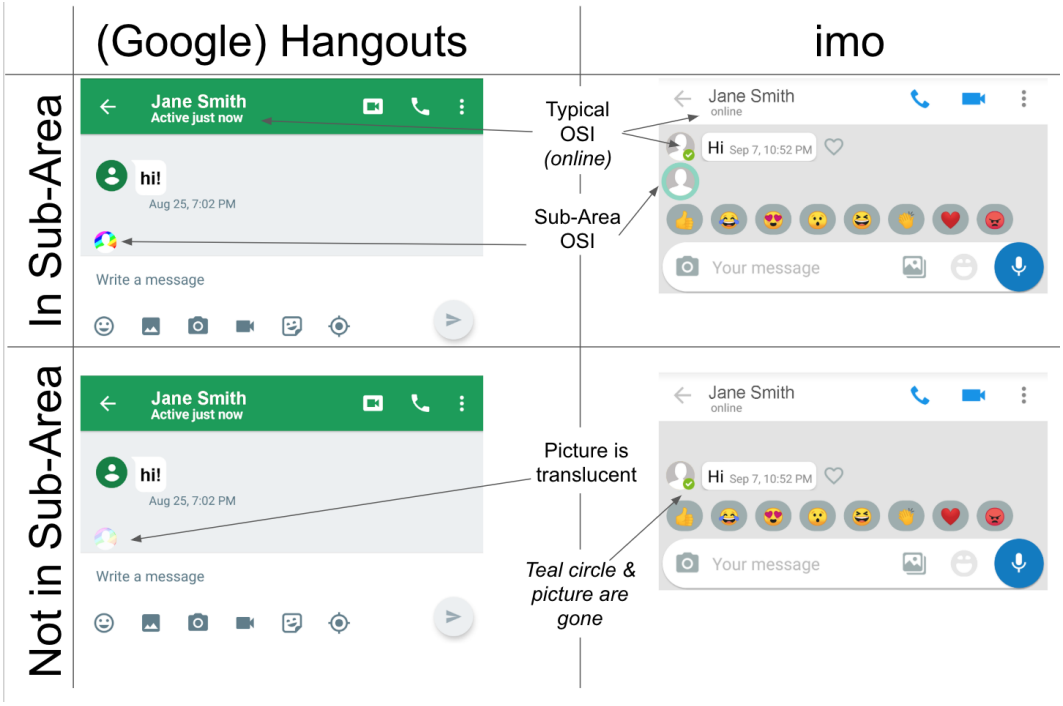


Figure 3.8: Hangouts and imo have separate OSIs with Typical scope and Sub-Area scope that shows other users' presence within a conversation.

observed user is accessing (*e.g.,* Facebook might show the user as "Active on Messenger" or "Active on Facebook").

3.4.5 Settings

All apps but LinkedIn have their OSIs turned on by default. As shown in Table 3.3, 20 provide settings that let users turn off or hide their OSIs, so that it no longer corresponds to their actual app/service use. This could mean that the OSI disappears completely, changes to show that the user has turned it off, or that the user appears offline permanently. Section 3.4.6 describes these differences in greater detail.

The design and implementation of OSI settings varies across apps, including similar apps made by the same company. For example, Figure 3.9 shows how users can update their OSI settings in 9 apps. OSI settings in Facebook (a) and Facebook Lite (b) are reached through similar but not identical settings menus; users reach the equivalent setting in Facebook Messenger (c) by clicking the green dot in a non-menu interface. Waze (d) is the only app for which a toggle is turned *on* rather than *off* to prevent others from seeing online status updates. LinkedIn (f) is the only app that explicitly prompts users to notice OSIs and consider changing their settings; however, as previously noted, this cue is accompanied by an automatic change to make the OSI visible to connected users. WhatsApp (i) has an option labelled "Last Seen" in its privacy settings, but this determines only whether the last online time is shown; it is not possible in WhatsApp to prevent others from seeing whether you are *currently* online. This may be especially confusing to users since four other apps (Hike (h), Hangouts, imo, and Telegram) also have a "last seen" setting, but these *do* turn off OSIs.

Locating OSI Settings

An imperfect measurement of how easily discoverable these controls are is the number of clicks it takes upon opening the app to turn off OSIs. This number ranges from 3 to 6, though in some cases (*e.g.,* Facebook) the count is significantly higher than the number of

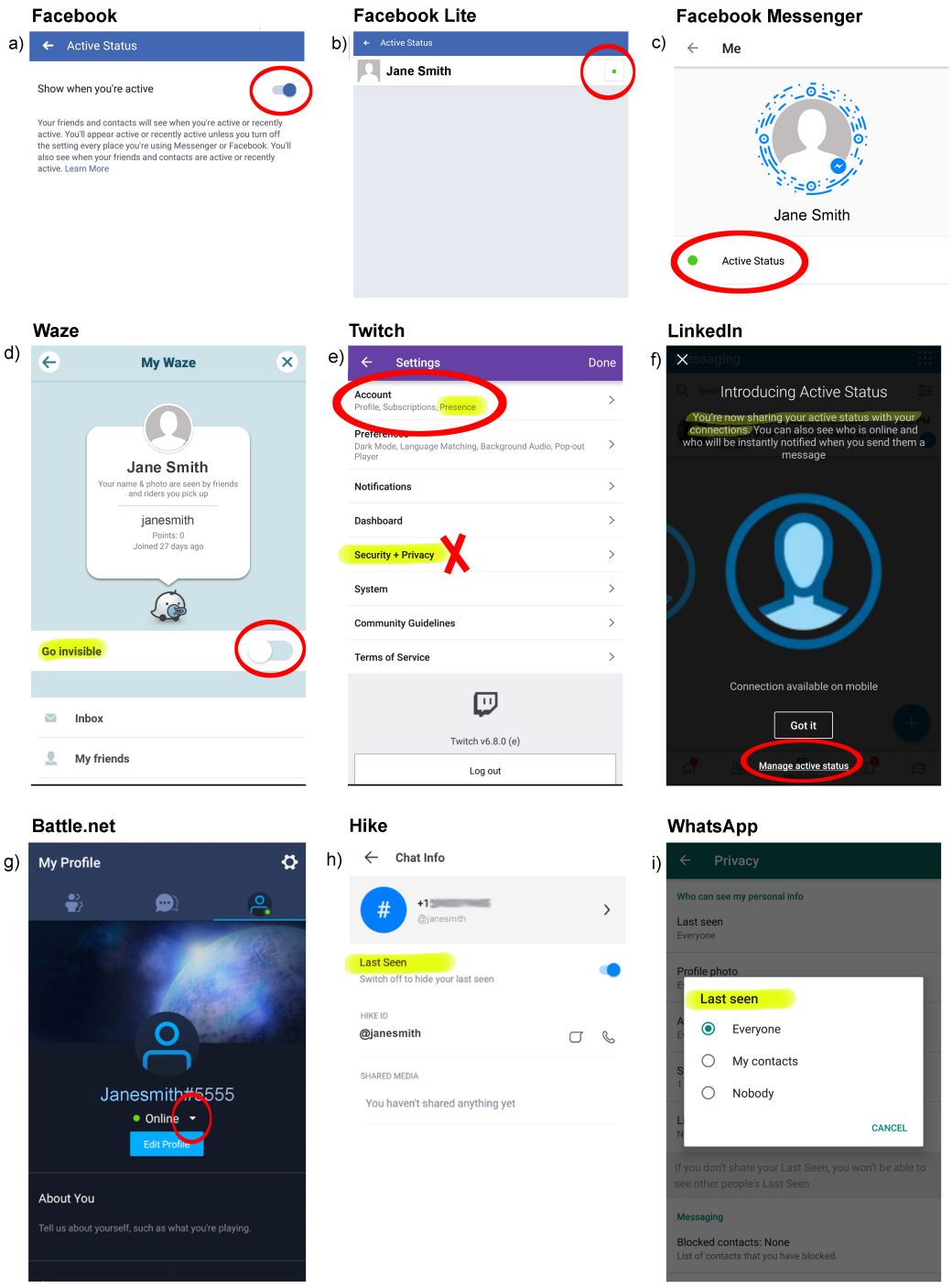
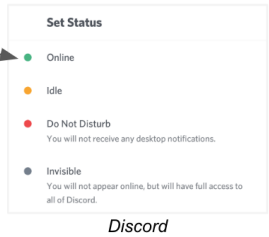
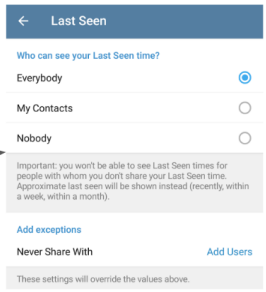


Figure 3.9: Screenshots related to OSI settings in a variety of apps.

APP	CLICKS TO TURN OFF ONLINE STATUS (excluding scrolling)	RECIPROCITY	AUDIENCE OPTIONS	AVAILABILITY OPTIONS
Battle.net *	3	No		Online, Away, Busy, Appear Offline
Discord	3	No		Online, Idle, Do not disturb, Invisible
Facebook	6	Yes		
Facebook Lite	5	Yes		
(Google) Hangouts **	5	No		
Hike	5	Yes	Everyone, Friends and Contacts, Friends, Specific People, Nobody	
imo **	4	No	Everyone, Contacts, Nobody	
Instagram	5	Yes		
LinkedIn	5	Yes	All LinkedIn Members, Connections Only, Nobody	
(Facebook) Messenger	4	Yes		
(Facebook) Messenger Lite	5	Yes		
Skype	3	No		Active, Do not disturb, Invisible
Slack	3	No		
Steam	3	No		
Telegram	5	Yes	Everybody, Contacts, Specific People, Nobody	
Tumblr	5	No		
Twitch	4	No		Online, Busy, Invisible
Viber	6	Yes		
Waze	3	No		
WhatsApp Messenger ***	6	Yes	Everyone, Contacts, Nobody	



Discord



Telegram

* OSI settings in Hearthstone are propagated via changes to settings in the Battle.net app

** Only applies to typical OSI for this app; sub-area OSI does not have settings

*** Online status cannot be turned off in WhatsApp; this row refers to the "Last Seen" setting in WhatsApp

Table 3.3: Properties of apps with OSI settings.

clicks it would take to *find* OSI settings because the app requires users to click through dialogues to confirm that they actually want to turn off OSIs. The location of controls for OSIs within the app, particularly in relation to privacy settings, may also contribute to how discoverable the controls are and may suggest whether companies view online status as carrying potentially sensitive information. Of the 18 apps that let users change their *Typical* OSI settings within an app, the settings for 9 apps can be found in a "privacy" menu or list. In Twitch, users must choose a menu option labelled "account" *instead* of "privacy" to find online status settings (Figure 3.9 e). Battle.net, on the other hand, lets users change their OSI settings directly from their profile via a small arrow next to the OSI icon rather than navigating through menus at all.

Controlling OSI Audience or "Availability"

Four apps (Hike, imo, LinkedIn, and Telegram) let users specify the audience for their online status in terms of relationship, specifically choosing from groups listed in Table 3.3. Hike and Telegram further enable users to specify which *individuals* can or cannot see their online status updates. The browser version of Facebook *does* let users control OSI visibility for specific subsets of friends, but this is not the case for the Android or iPhone Facebook apps. Four other apps allow a greater range of expression in terms of availability (*e.g.,* "away," "busy," or "appear offline" in Battle.net), shown in Table 3.3.

Do OSI Settings Propagate?

Whether settings propagate across related apps can make cross-app OSIs especially difficult to reason about. Hearthstone's OSIs cannot be turned off within the Hearthstone app, but they *can* be turned off by turning off OSIs in the Battle.net app (thus, the settings propagate between apps). When users turn off Facebook app OSIs an explicit policy informs them that settings are separate for each app and/or device. That is, settings *do not* propagate across apps or devices for Facebook. Online status in Slack must be turned off separately for each "workspace" but *does* propagate across devices. Although I restricted the scope of my study

to mobile apps, the question of OSI setting propagation between mobile and desktop versions of the same app could lead to even more cognitive load for users who want to control their presentation-of-self via OSIs on multiple apps and devices.

Reciprocity

For 10 apps with OSI settings, users can still view others' OSIs even if they have turned off their own (*i.e.,* the app does not provide *reciprocity*), as shown in Figure 3.10. Viber, which has reciprocity, lets users change their online status setting only once per 24 hours. While this nudge toward authenticity may discourage toggling the setting to spy on others, it could cause users to be temporarily stuck with settings they did not intend. Related to the reciprocity of the "last seen" setting in WhatsApp, Buchenscheit et al. found that participants were hesitant to turn off their own "last seen" because they wanted to see others' [37]. Thus, reciprocity of OSI settings could result in coercive contracts in which users who wish to view the OSI of someone who *is* willing to share it can do so only by compromising *their own* privacy preferences.

3.4.6 Observed OSI Compared to Ground Truth User Behavior

OSIs are not always faithful representations of a whether a user is *actually* online or offline. Disconnects between people's OSIs and their actual behavior may be caused by users setting their OSI to offline or by latency in updates to an OSI as users come online or go offline. An adversary might want to learn the conditions under which they can "trust" an OSI's accuracy and/or calculate a more accurate representation of target users' actual app use. It is not my goal to support this adversarial use-case; instead, this section draws attention to ways that OSI design might hinder or support malicious actors. Additionally, understanding these conditions could help potential victims be aware of adversarial capabilities and understand situations in which they can or cannot hide their app usage patterns. App use on non-mobile devices, which was out of scope, may introduce additional situations in which OSIs do not precisely reflect actual use, some of which are discussed in Section 3.7.4.

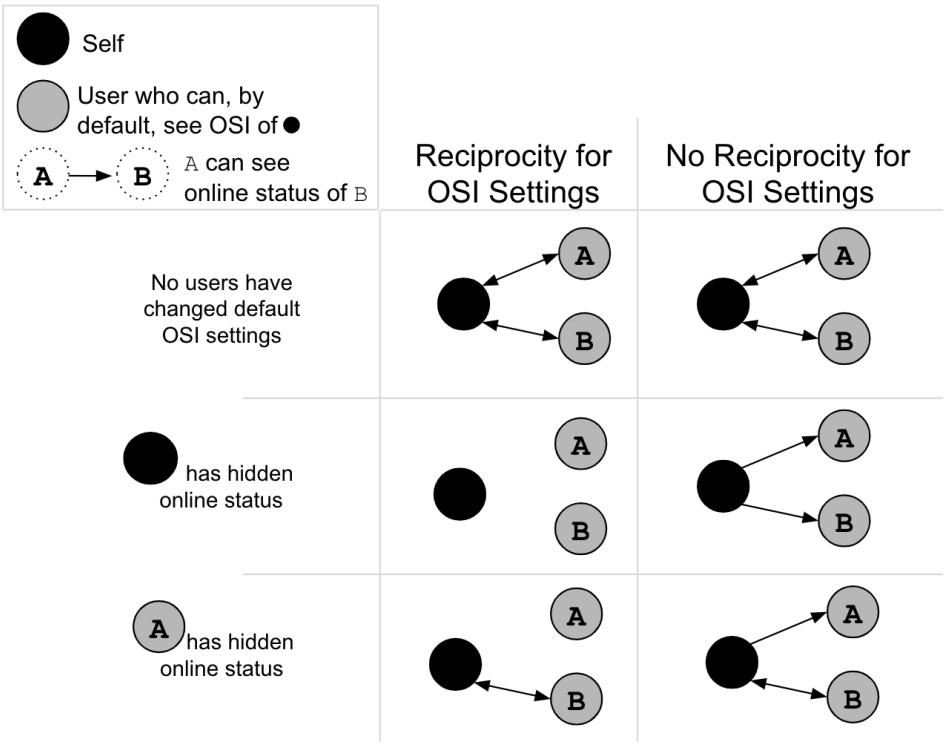


Figure 3.10: Reciprocity of OSI settings means that a user cannot see others' OSIs if they choose to turn off their own.

Time to Appear Online/Offline

The granularity with which an adversary could monitor someone's app use is related to the typical *amount of time* it takes for users to appear online or offline *and* the *consistency* of this timespan. I report the time to appear as online or offline in coarse-grained buckets in Table 3.2. For all apps, the OSI updates as fast or faster when users come online compared to when they go offline. In most apps and for all Sub-Area OSIs, an adversary could determine actual app use with a precision of just a few minutes or better.

Consider Hangouts as a concrete example of how an adversary might leverage timing and consistency information to track a target user's app use. Users appear online almost immediately and appear offline 15 minutes after they stop using the app. An adversary would know that observed users were *actually* online around the time they came online and *actually* online approximately 15 minutes before their OSI changed to offline. If observed users appear online for an extended period of time, an adversary could determine that they were *actually* online at least once every 15 minutes in that period, though they cannot know exactly how many times or when users opened and closed the app.

As discussed in Section 3.3, an adversary who wants to monitor someone's OSI with the best possible granularity might need to take certain actions, like repeatedly refreshing the page in the app where the OSI appears or closing and re-opening the app. These added steps would not prevent a dedicated adversary (or an adversary who could automate OSI observation) from tracking someone, but they might discourage casual adversarial behavior. In this respect, Tumblr might be especially effective at discouraging adversaries. Its OSI decriptive text, while always technically correct, is phrased so that a single OSI observation provides only vague insight into a user's actual behavior; if the user is online, multiple refreshes of their profile can display either "Active in the last hour" or "Active in the last 2 hours."

Potential Detectability of Changing OSI Settings

Further exploring OSI trustworthiness, an adversary may wish to know whether their target has their OSI turned off. First, if turning off an OSI changes its appearance such that it looks *different* than if the user had their OSI on, it would be obvious *that* the user has changed the OSI setting, but potentially impossible to determine *whether* they are currently online. For example, it is clear in WhatsApp that a user has turned off the "last seen" setting because the area that normally shows their last online time will be blank when the user is offline (recall that it is not possible to turn off OSIs in WhatsApp, so online users will still appear as online). In apps where turning off an OSI causes the OSI to appear as though the user were offline, it would be harder but not impossible to detect *that* the user has changed this setting. Taking the previous example of Hangouts, although users consistently appear offline 15 minutes after they actually go offline, turning off the OSI causes a user to appear offline *immediately*. To ensure that others cannot detect when they turn off OSIs, users would need to stay online for 15 minutes before they actually change the setting while refraining from observable app activity.

Additionally, in either of the preceding cases, if users who have turned off their OSIs continue to interact with the app in ways that are visible to other users, those other users could infer that they have turned off their OSIs. For example, posting on Facebook while appearing offline lets friends detect that you have turned off OSIs; chatting with someone in a private conversation while appearing offline in the app lets that person know you have turned off OSIs.

3.5 User Survey Methodology

I next conducted an online survey, approved by the University of Washington's IRB, to contextualize the app analysis findings. I recruited 205 people on Mechanical Turk to complete the survey, all of whom had completed at least 1000 HITS with 98% acceptance rate and had not participated in any of my pilot surveys related to OSIs. I excluded 4 people's responses

Age	24 or under (25), 25-29 (45), 30-34 (43), 35-39 (31), 40-44 (16), 45-49 (16), 50 and above (20)
Country	United States (187), India (8), Other (5)
Ethnicity	White (158), Asian (18), Hispanic/Latino (9), Black/African-American (10), Other or Mixed (4)
Education	Bachelor's Degree (93), Some College (33), High School (27), Associate Degree (25), Advanced Degree (16), Trade/Technical School (5), Less than High School (1)
Gender	Male (115), Female (85)
Colorblind	No (198), Yes (2)

Table 3.4: Summary of survey participant demographics

because their answers suggested that they did not understand the survey and one person who submitted the survey twice. Thus, my survey had 200 responses. Participant demographics are described in Table 3.4.

Survey questions fell into 5 categories: (1) app use, (2) recognition of OSIs design patterns, (3) app-specific OSI knowledge, (4) ability to locate OSI settings, and (5) experiences with OSIs. Questions were asked in this order, and participants could not "go back" to previous survey pages. Demographic questions appeared at the end of the survey. I paid participants a base rate of $3 and bonuses as specified below.

3.5.1 App Use

I first asked users to mark which of 38 apps they used; this included all of the apps I identified as having OSIs *except* for Facebook Messenger Kids (since I did not expect kids to participate) and, by oversight, JOYRIDE Dating.

3.5.2 Recognition of OSI Design Patterns

I then performed a between-subjects experiment. The purpose of this experiment was to understand whether users recognize common OSI design patterns (*e.g.,* dot icons) and how other OSI components, like additional context or color, affect users' recognition and understanding of OSIs. Each participant saw a series of 5 images that contained increasingly contextualized abstract components of OSIs, as shown in Figure 3.11. Participants were randomly assigned to experimental groups; a control group (56 participants) saw these images in gray scale. Although I specified that the images were in gray scale, some participants' responses suggest that they interpreted meaning from the gray color of the dot. For other groups, I varied the color of the abstract OSI components to green (50 participants), orange (41 participants), or blue (53 participants).

For each image, participants were asked to provide an open-ended response to what they thought the dot meant. One researcher coded all responses to determine if participants had correctly determined that the dot was an OSI. I coded 10% of the responses for agreement and calculated a Cohen's Kappa score of k=.94 for our agreement. We considered participants' responses to be correct if they identified that the dot meant that the person was online or available or that it represented an online status indicator even if they did not specify that the indicator conveyed that the person was currently online. We separately coded 107 responses that we considered partially correct. These included responses where participants offered multiple explanations for the possible meaning of the dot and cases where participants understood that the dot was an OSI but believed that it indicated that the person was *not* currently online.

After they had seen the full progression, I asked participants if "Oprah Winfrey" (whose name and photo appeared in the images they saw) is currently using the app based on the final image. Participants were given a chance to submit open-ended comments about their experience answering the previous questions.

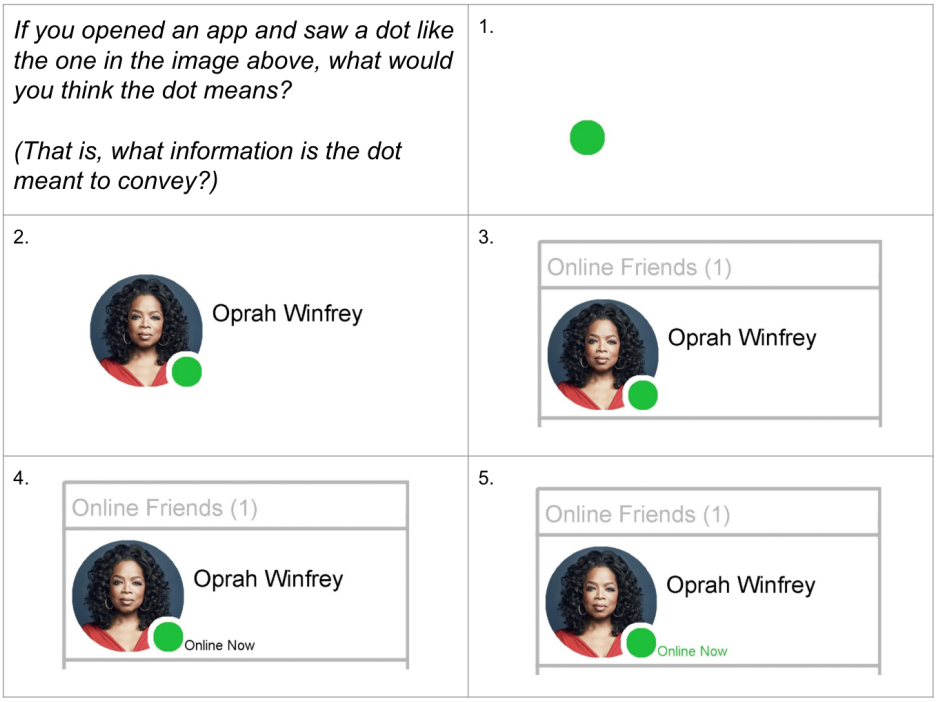


Figure 3.11: In the experimental component of my survey, participants saw this progression of images and, after each image, answered the question in the top left. A control group saw these images in gray scale, and other groups saw the images with OSI components' (dot and "online now" text) in green (as in this figure), blue, or orange.

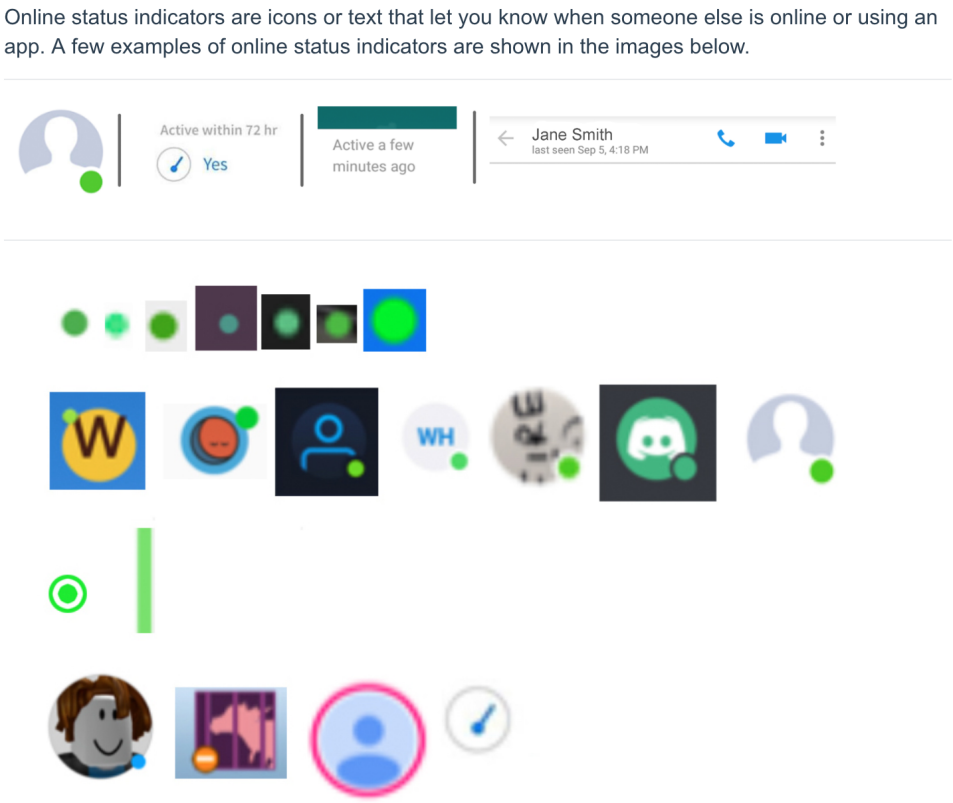


Figure 3.12: This image and explanation was shown to participants to minimize the possible impacts of which experimental condition they experienced in the previous section of the survey.

3.5.3 App-Specific OSI Knowledge and Ability to Locate OSI Settings

Next, so that participants were on an even footing going forward in the survey, I explained what OSIs are (Figure 3.12). For each app they previously reported using regularly, I asked participants to answer whether it had OSIs, without looking at their phone.

Then, for apps they use regularly, I asked participants to open the app on their phone and time themselves to see how long it took to find OSI settings (Figure 3.13). Participants received a $0.50 bonus for each app they reported timing. I did not ask participants to actually change their settings, only to find them. The phrasing of these instructions was important. Since we asked participants to "find the settings to turn off online status (that is, settings to make yourself appear offline to other users, even when you have the app open)," the "last seen" setting in WhatsApp does not meet this criteria. I cannot know whether participants who reported that they found this setting in WhatsApp misunderstood the setting in WhatsApp or did not notice the nuance of my phrasing. After completing this task, users could enter free-response comments about the process of looking for settings, including "what [they thought] made some apps easier or harder, if [they] found the settings but [were] still not sure how they work, or something else."

I conservatively excluded all timing data reported by 33 participants whose answers or free-response explanations made me doubt whether they had actually completed the task. I obtained 683 timing reports from 154 unique users representing 35 apps. I asked participants to report how confident they were that they had found the correct settings or that the app did not have OSI settings on a scale of 1 to 5. This was a useful attention check; however I did not use the certainties in my analysis of responses. I consider each timing report as independent and do not consider within- or between-user patterns. I analyzed and identified themes in the open-text responses related to the timing task, including responses from participants whose timing reports were excluded.

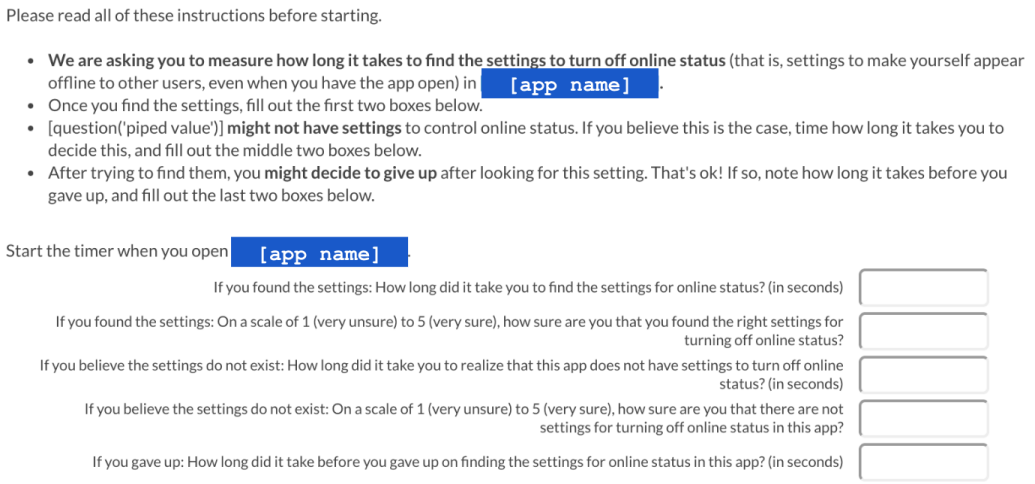


Figure 3.13: I asked participants to measure how long it took them to turn off OSIs in apps that they use regularly and how certain they were that they had found the settings (or that the setting did not exist) on a scale of 1 to 5.

3.5.4 Experiences with OSIs

To generate free-response prompts for the survey, I recruited 17 security and privacy professionals to participate in an expert panel exercise to build user scenarios during a regularly scheduled tech policy discussion group. The panel generated scenarios in which users' experiences with OSIs might have security or privacy implications and then clustered these scenarios through an affinity diagramming exercise. One representative from the panel worked with researchers to generate 5 survey prompts, phrased as yes/no questions in Figure 3.14, such that all clusters of scenarios could have been a plausible response to at least one of these prompts. In addition to answering the yes/no questions, I invited participants to answer free-response prompts describing a related personal experience. Participants could enter free-response answers regardless of how they answered the questions above. I included one additional chance for participants to "describe any other noteworthy experiences" they had with OSIs. I paid a bonus up to $2 for answering free-response questions.

Two researchers independently identified themes in the open-text responses to these

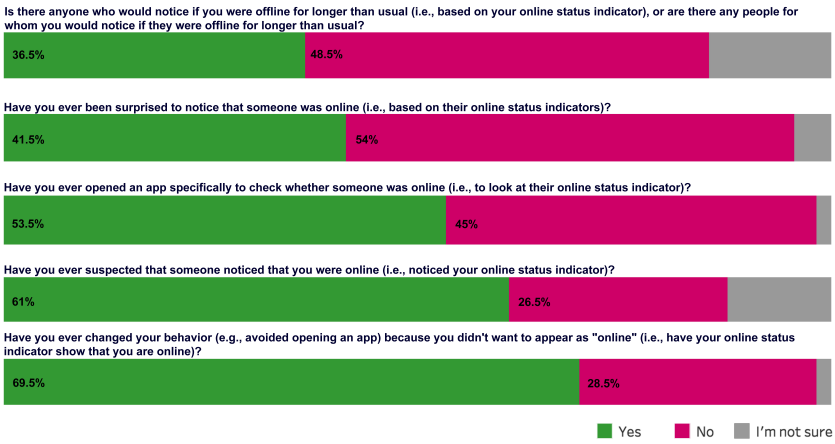


Figure 3.14: Through an expert panel of security and privacy experts, I developed 5 prompts to inquire about participants' experiences with OSIs. For each prompt, at least 35% of participants expressed that they had this experience.

prompts and then discussed the responses to agree on a set of themes for coding. One researcher coded responses based on the agreed-upon themes.

3.6 Survey Findings

3.6.1 App Use

Figure 3.15 shows the number of participants who reported regular use of each of the 38 apps I included in the survey.

- Instagram and Facebook are both used by over half of participants, and 5 other apps are used by at least 25% of participants. Only two participants said that they do not regularly use any of the apps.

- Many participants use more than one app that has OSIs; the median number of apps participants used was four, and two participants used 15 of the apps I studied. Using more than one app with OSIs may increase the total amount of a person's time that

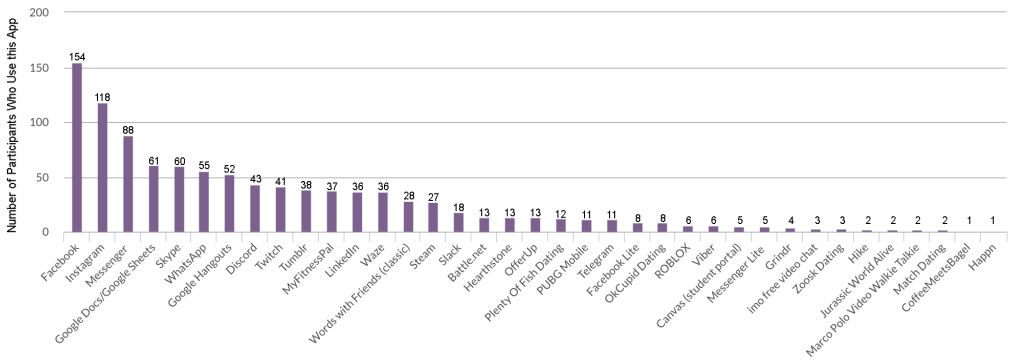


Figure 3.15: The number of participants who reported that they regularly use each app in my survey. All of these apps have OSIs.

can be monitored via OSIs and may enable adversarial monitoring abilities beyond what is possible within a single app.

- Because some apps are especially popular, the design patterns in those apps may be more prevalent in terms of recognizability than in terms of the actual percent of apps that use this design pattern. This is shown for several design patterns in Table 3.5. For example, although half of the apps I studied do not provide settings to avoid appearing online, only 67.5% of participants regularly use apps without these settings compared to 97.5% of participants who regularly use at least one app with OSI settings.

3.6.2 Recognition of OSI Design Patterns

The results of the experimental component of my study designed to evaluate users' recognition of OSI design patterns (Figure 3.11) are shown in Figure 3.16. As each participant saw a dot of a single color surrounded by progressively overt visual cues indicating the dot represents an OSI, I first evaluated, for each person and for each cue, whether the participant accurately understood the purpose of the UI as an OSI. I next calculated a cue-number score

	% (count) of participants who ...	Use at least one app with ...
OSIs in general	99% (198)	OSIs
Icon appearance	96.5% (193)	Green dots
	34.5% (69)	Variations of green dots
	72.5% (145)	Something other than green dots
Existence of OSI settings	97.5% (195)	OSI settings
	67.5 (135)	No OSI settings
Implementation of OSI settings	94.5% (189)	Reciprocity if OSIs are turned off
	68% (136)	No reciprocity if OSIs are turned off
Default OSI audience	53% (106)	Global Default OSI Visibility
	98.5% (197)	Default OSIs visible to only connections

Table 3.5: Percent and number of participants exposed to varied design patterns identified in app analysis, based on the apps they report using regularly. For example, the first row in "icon appearance" denotes that 96.5% of participants use at least one app with green dots.

for each participant, that is, the earliest cue at which the participant understood the UI to be an OSI.

A one-way ANOVA with condition (*i.e.*, whether they saw a dot rendered in green, blue, orange, or gray) as the independent variable and cue-number as the dependent variable revealed a highly significant difference by color, indicating a significant difference in the number of cues an individual needed before they recognized a dot as an OSI, depending on the color ($F(3,160) = 12.640$, p ¡ .001). *Post hoc* analysis revealed that participants who saw a green dot required significantly fewer cues (mean = 1.96, sd = 0.89) than participants who saw a blue dot (mean = 2.77, sd = 1.00, $t(87) = -4.05$, $p = .001$), gray dot (mean = 2.89, sd = 1.00, $t(88) = -4.67$, p ¡ .001), or orange dot (mean = 3.19, sd = 0.91, $t(75) = -5.92$, p ¡ .001). There were no significant differences between other groups. A Bonferroni correction was applied to all comparisons.

I next examined the cumulative impact of each of the visual cues I provided (*i.e.*, the five progressive images in Figure 3.11 and on the x-axis of the grey graph in Figure 3.16). A Cochran's Q test comparing participant understanding at each of the five levels of visual cues (collapsing across all conditions) revealed a highly significant difference between levels

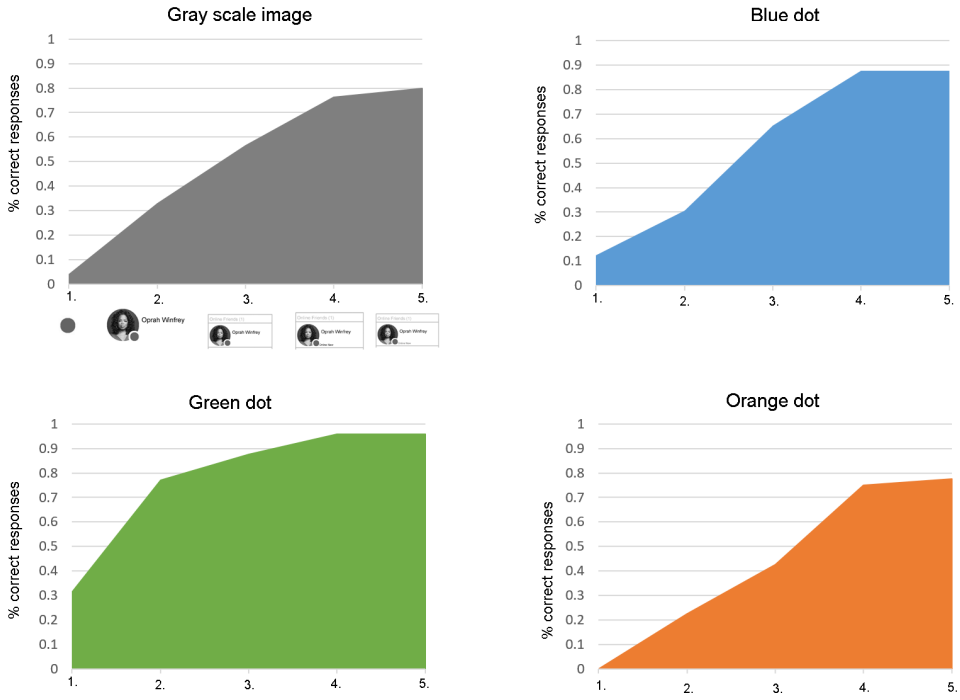


Figure 3.16: Results of the experimental component of my survey, which demonstrate that participants are more likely to recognize green dots being used as OSIs and that contextual cues helped them understand OSI icons even if the icon was a less typical color.

($Q(4) = 398.9$, p ¡ .001). *Post hoc* comparisons revealed a significant jump in participant understanding between each pair of successive levels, except for levels 4 and 5, where I saw no significant difference. Thus, each of the first four visual cues increased participants' likelihood of interpreting the image as an OSI when they were added to the interface.

3.6.3 App-Specific OSI Knowledge

Almost all participants (198 of 200) reported regular use of at least one of the apps I studied, but they were not always aware that these apps have OSIs.

- Participants answered "Does [app name] have OSIs?" 1,021 times for apps that they used regularly. Of these reports, 635 (62%) correctly identified that the app had OSIs.

Although 89.5% of participants (179) correctly identified that at least one of these apps had OSIs, 62.5% of participants (125) answered that they were not sure if the app had OSIs for at least one app. 35.5% of participants (71) answered incorrectly for at least one app when asked if it had OSIs (i.e., wrongly believing that it did not).

- Incorrect answers and uncertainty were not evenly distributed across apps, as shown in Figure 3.17 for apps used by at least 10% of participants. For example, most participants correctly identified that (Facebook) Messenger and Discord had OSIs, but only a few knew that MyFitnessPal had them. Some differences may be related to how OSIs are designed in each app. For instance, OSIs on Instagram are only visible between users of the messaging feature, so it is plausible that responses for Instagram correlate with whether each participant uses that feature.

3.6.4 Locating OSI Settings

I asked participants to open each app they used regularly and find the settings menus that would let them adjust their OSI.

- They reported locating these settings in the majority of cases (64% of all reports; 72% of reports for apps with OSI settings).

- Of the reports for apps with OSI settings, so out of only 524 total reports, 28% of the time participants were unsuccessful and gave up before finding the relevant settings. Success was not uniform across apps, with some creating more of a struggle than others; for example, only 58% of participants found the OSI settings in Instagram, and the average time to find OSI settings was highest in LinkedIn (90 seconds spent looking for settings in LinkedIn compared to 48 seconds in Instagram).

- In apps that lack OSI settings, participants mistakenly thought they had found OSI settings in 23% of cases. Half of these false positives occurred in WhatsApp, where

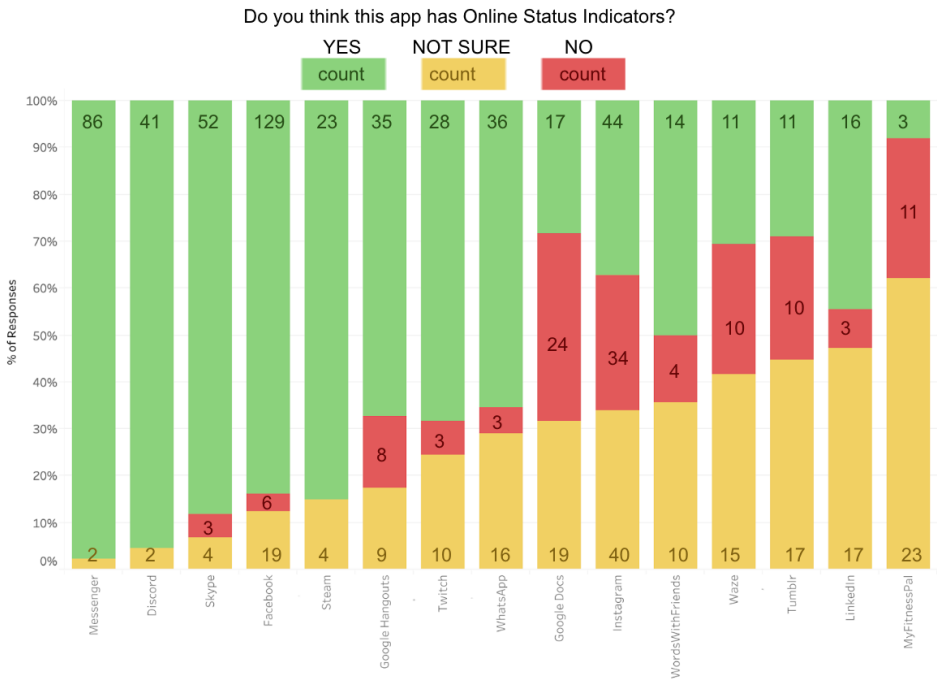


Figure 3.17: For apps used by at least 10% of participants, this graph shows what percent of respondents believed that the app did or did not have OSIs. For 10 of the 15 apps shown in this figure, more than 30% of participants did not answer correctly that the app has OSIs.

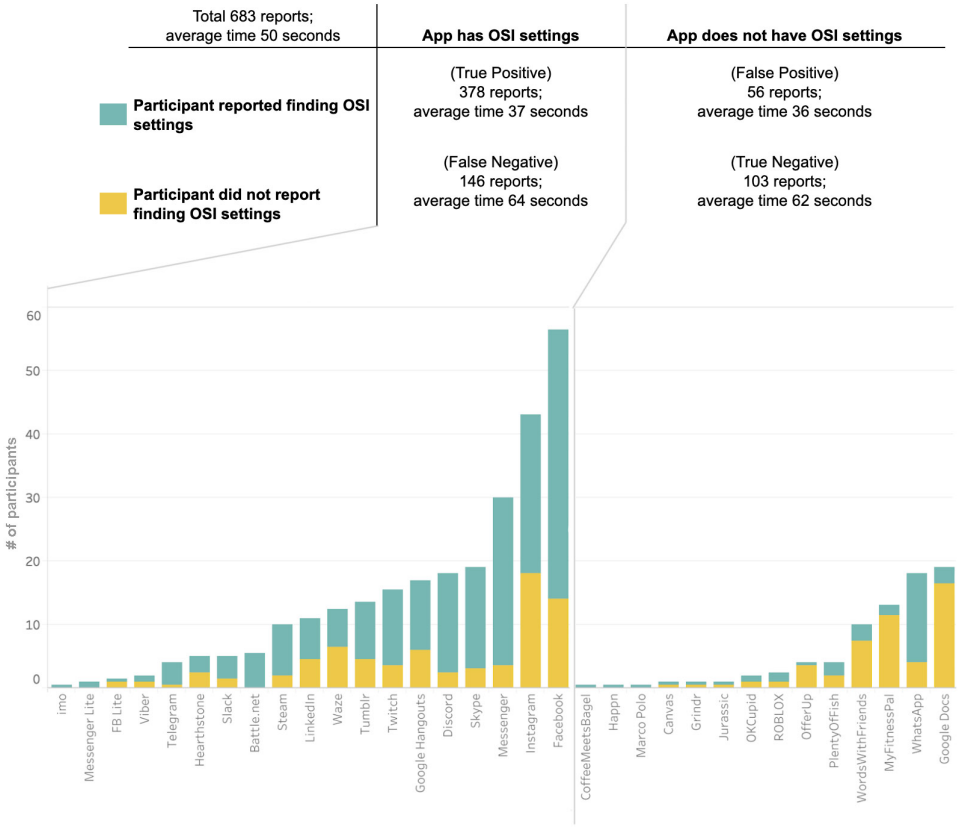


Table 3.6: This table summarizes the results of 683 instances where participants reported the time it took them to find (or give up on finding) OSI settings in an app in terms of the number or false/true positives/negatives and the average time participants spent looking for OSI settings.

participants were particularly likely to be misled into thinking they had found an option for turning off their OSI.

In response to an open-ended prompt, participants described their experience performing this task. P132 summarized a feeling that many other participants shared, saying: *"It was super annoying to look for some of these, it should be way easier."* Forty participants proactively mentioned expecting to find the OSI settings in the settings menus, though many described difficulties locating or navigating these menus. For example P145 said, *"For the*

apps that don't put them in settings it can be a little difficult to maneuver and try to find exactly where to turn it off."

Participants frequently reported that these settings were not sufficiently prominent. Even after locating the broader settings menu in which these options were embedded, some participants still expressed frustration finding OSI settings, saying things like: *"There are a lot of different privacy settings and it was difficult to figure out which link led to which settings"* (P19). Three participants hypothesized, unprompted, that app designers intentionally make OSI settings hard to find. For example, P188 stated: *"I would venture to guess that most of these apps make it hard to find the settings to change online status because they want it to seem like all of your friends are using the app at all times."*

Ten participants spontaneously expressed that controls to adjust an OSI should be separate from the settings menus. These participants said they looked for OSI settings near their profile picture or in a place where their own OSI was visible. P64 drew direct attention to the fact that not all apps have self-visibility of OSIs: *"I think the apps that made it obvious you were online or offline from the beginning made it easiest."*

Finally, although many participants found this task challenging, even those who found it straightforward at times overestimated their understanding of the interface. Several participants expressed incorrect beliefs about how settings propagate across devices or apps; in particular, three users incorrectly stated that turning off an OSI in the Messenger app would disable it in Facebook, as well: *"For facebook, it was really easy. I just had to check messenger settings and I found it easily"* (P46).

3.6.5 Experiences with OSIs

Several themes emerged through users' stories about their experiences with OSIs. Here, I describe three common themes that cut across the prompts I used to solicit users' experiences.

Efforts to Control OSIs

Many participants reported wanting to control how their OSI appears to others. They cited a variety of ways in which they alter their behavior to manage their OSI, reasons for wanting to appear offline, and audiences for whom they cared about appearing as offline. Forty-six participants (23%) said that they had changed their OSI settings, suggesting that participants independently discovered and used OSI settings. However, even more participants (37%) said that they self-regulated their use of an app, for example, by avoiding opening the app or by signing out quickly if they saw someone online with whom they did not want to speak. P27 described the meticulous process he uses to control how his OSI appears to his ex: *"[She] would notice if my online status is irregular or weird. That is why even though I am online in invisible mode, I would keep a schedule of being visible so I do not rouse suspicion from her."* Three participants deleted an app from their phone altogether specifically to avoid appearing online. That so many participants reported changing their behavior to use apps in non-preferred ways (occasionally abandoning the app altogether) points to a failure for apps to robustly support users' privacy preferences.

Participants also described instances where controlling their OSI was difficult in other ways, as well. P22's frustration with appearing online in Skype while only intending to check email corroborates my observation from Section 3.4.4 that cross-app OSIs may make it especially difficult for users to anticipate how they appear to others: *"Sometimes it doesn't make it too clear if someone is really online on a chat portion of an app, rather than just on a related site . . . I used to log into my email just to check that, and it would automatically log me into the chat which was connected to skype — which was something I was NOT expecting it to do, and which made me feel bad if people tried to message me while I was really not able to talk."* P187 also described frustrations with OSI settings that he struggled to reign in: *"Some of them save your setting for the next time that you open the app or login, which is nice. However, others will forget your setting and show you as 'online' until you change it to the one that you want. Other apps also will 'clear' your status and cause you to be shown*

as 'online' if you make any action that can be described as being 'active' which is also not desirable."

Like P27, 85 other participants (43%) discussed updating OSI settings or changing their behavior because they were trying to avoid a *specific* person. Only 50 participants (25%) said that they wanted to avoid people (or friends) in general. Since the only apps in my analysis that support the ability for users to hide their OSIs from specific other users are Telegram and Hike (used by only 11 and 2 participants, respectively), participants who expressed this preference likely found that the apps did not support this goal.

I also examined *why* participants wanted to appear offline; 27 people (14%) said they were busy and just did not want to be bothered or distracted. Of the participants who wanted to avoid a specific person, 21 (24% of the 86 people avoiding someone in particular) said they were not ready to respond to a message that someone had sent them. Others were avoiding someone who habitually annoyed them online, someone with whom they had a conflict in "real life," or people who know them in a specific capacity (*e.g.*, work colleagues). Twelve participants (6%) stated that they wanted to appear offline to avoid being caught in a lie. For example, P137 describes: *"I have been chatting with a friend on Facebook and told her I needed to get off to go to bed. Once I got in bed, I wanted to check something on Facebook, but I did not want to appear as if I had not been truthful to her."* This story illustrates a common theme of users feeling this tension even when the "lie" is a white lie or represents a change of plans.

Observing Others' OSIs

Sixty-one percent of participants (122) reported that they had, at some point, suspected that someone else noticed their OSI. Articulating why they believed this, 18 said they were told directly by the other person, *"I saw you were online"* (P157). Many participants had received messages that they inferred had been sent *because* the other user saw they were online. For 43 participants, these messages came shortly after they came online, including P45, who said, *"Someone messages me soon after I've gone online — too soon for it to be a coincidence."*

P57 had a similar experience and described that the she felt like, *"the indicator has blown my cover."* Twenty-seven participants described receiving messages while they were online, though not necessarily shortly after signing on: *"I have received creepy messenger messages from strangers when I've been online — it seem[s] to only happen when I'm online and not offline"* (P148). In some cases, users received messages that they believed were sent because they had been offline for an extended period, which suggests that others notice patterns in online status. For example, P29 wrote: *"My friends and family would check up on me if they didn't see me online for more than a week or so. I know this because they send me messages asking if I'm okay when I'm on vacation or what not."*

Many participants also described noticing someone else's OSI. Eighty-three participants reported they had, at some point, been surprised to see someone online, and over half of survey participants (107) reported opening an app *just* to check someone's OSI. The scenarios in which participants noticed or looked up someone's OSI provide insight into the types of inferences that users, especially people who know each other, might make based on each others' OSIs. In particular, participants made inferences about others' availability for communication, feelings or reasons for not replying to messages, and real-world behavior or wellbeing.

Participants explained that they were surprised to see someone online because: they expected the person would have been asleep (17 participants), the person had not been online in a long time or does not come online often (14 participants), the person implied they were going offline or would not be online (13 participants), or they expected or knew that the person should have been at work (7 participants). Though some participants gave others the benefit of the doubt and believed that seeing them online unexpectedly was caused by a change of plans (7 participants) or a bug in the app (3 participants), others believed that their friend had lied (6 participants) or held a negative view without confronting them (6 participants). P28 described using OSIs to catch their partner in a lie: *"My boyfriend at the time said that he had lost his phone. I was on facebook that day and he was online. He doesn't have a laptop or ipad so I knew that he had lied about loosing [sic] his phone. He was*

busted because I seen he was online."

Many participants said they would use OSIs for practical, typically benign purposes, such as trying to figure out if it is a good time to contact someone, to figure out the best way to contact someone (*e.g.*, Facebook message versus a phone call), or because they were hoping to interact with a specific person (*e.g.*, play games or start a synchronous conversation). For example, P156 said, *"Sometimes I check to see if my mother or sister have been online if it's early in the morning or late at night. That way I know I can text them without waking them."* A few participants expressed less definitively practical reasons for looking up someone's OSI: trying to figure out if the person was ignoring them or "had a chance to read their message," or just trying to figure out if the person was active in general. For example, P54 looked up an OSI that includes a "last seen" feature: *"If they had been [online], it usually made me wonder why they hadn't responded yet."*

(Potentially) Adversarial Use of OSIs

Some participants described experiences with OSIs that seemed to be especially toxic. Participants described potentially harmful situations such as (perceptions of) "tracking" or being "tracked" via OSIs, and confrontations stemming from observations of OSIs. For example, P28 described looking up her son's online status: *"When I can't reach my son, I look on Facebook to see if he is online. He gets in trouble for not answering me but is sitting on his phone."* P133 was confronted by a friend who had noticed that P133 was frequently playing video games: *"I had a friend message me to tell me they thought I was playing video games too much. I was offended by this and left my status as offline permanently after this situation."*

Many of the other quotes I have already included throughout Section 3.6.5 focus on conflicts in romantic partnerships. Although I believe that many of these stories show the potential for OSIs to play a role in abusive relationships, I resist labelling any of these stories as "abuse" and instead provide quotes with minimal additional commentary.

3.7 Discussion and Design Recommendations

3.7.1 OSIs: Leaving Users App Dependent Rather than App Enabled

I found that participants struggled to manage the cognitive load of understanding what their OSIs broadcast about them and when. Their descriptions reflected misunderstandings about the interface and uncertainty about their audience. And the diversity of design decisions across apps led to vast inconsistencies in the way users' activity was represented and shared. When users explicitly attempted to turn off their OSI, they routinely found they were unable to do so or thought that they did so, but in fact did not.

Yet, despite this complexity, participants frequently conveyed that they care about what they project — and to whom — through OSIs. They value the ability to manage the appearance of their online activity, and they want their OSIs to reflect the usage patterns they choose to project. Whether hiding from a friend who is owed a reply, giving off the appearance of sleeping through the night, or remaining consistent in a claim of being unavailable, participants routinely behave in ways that will project carefully thought-out OSI presentations. In some cases, participants reported adjusting the interface of an app to align with the image they want to project, for example, using app settings to appear offline. But more often, participants described adjusting their behavior, making decisions about what to do based on the way it would be reflected through their OSI.

Prior work in HCI distinguishes between instances where users are *app enabled*, that is, provided with tools for pursuing new courses of action, and instances where users are *app dependent*, that is, restricted in their behaviors in a way that is determined by an interface [59]. In this study, I find that current OSI designs frequently leave users app dependent, and I see them adjusting their behaviors to manage what is displayed by their OSI, foregoing app use to maintain the outward perception that they are asleep or staying online to give the impression of being at work. These findings point to a need for OSI designs that are less likely to restrict and dictate users' behaviors, the hallmark of app dependence as defined by Gardner and Davis. Goffman's dramaturgical analysis informs us that users

will work to present themselves strategically to others online [61]. Knowing this, designers can either support this image management or lead users to contort their activities to produce the desired OSI presentation.

3.7.2 Re-imagining OSIs

Since participants described many beneficial uses of OSIs, how can we re-imagine them such that they continue to provide those advantages but are more difficult to leverage adversarially and less likely to lead users to allow an app to dictate their behavior? I see potential for future work to advance a research agenda around OSI design through provocative concepts and non-traditional OSI presentations. For example, current OSI designs support the potentially toxic behavior of obsessively checking and tracking another user's OSI. The ability to do this covertly could be minimized by creating a query-able OSI that allows users to view a record of who accessed their OSI and when. If an app requires users to actively seek out OSI information (rather than noticing it casually while using the app), it would be possible to apply rate-limits to the frequency with which a person could view someone's online status or the amount someone's online status could be viewed by others.

Letting users choose a schedule for when they should or should not appear as online, letting users appear online at random intervals, or letting users continuously appear *online*, even while offline, could support some known user needs and flush out other undocumented ones. Notably, a third-party service could approximate this functionality without requiring buy-in from app developers. These ideas would potentially undermine beneficial aspects of OSIs, but researchers might find that users are willing to sacrifice some of these benefits for the plausible deniability they would afford. I propose that a third-party OSI manager could enable users to manage OSIs across multiple apps and/or accounts (Figure 3.18 a).

Finally, given that participants in my study sometimes avoided opening an app because they did not want to appear online even long enough to change their OSI settings, researchers might explore whether a feature that lets users choose whether to appear as online each time they open an app (Figure 3.18 b) could decrease app-dependent behavior.

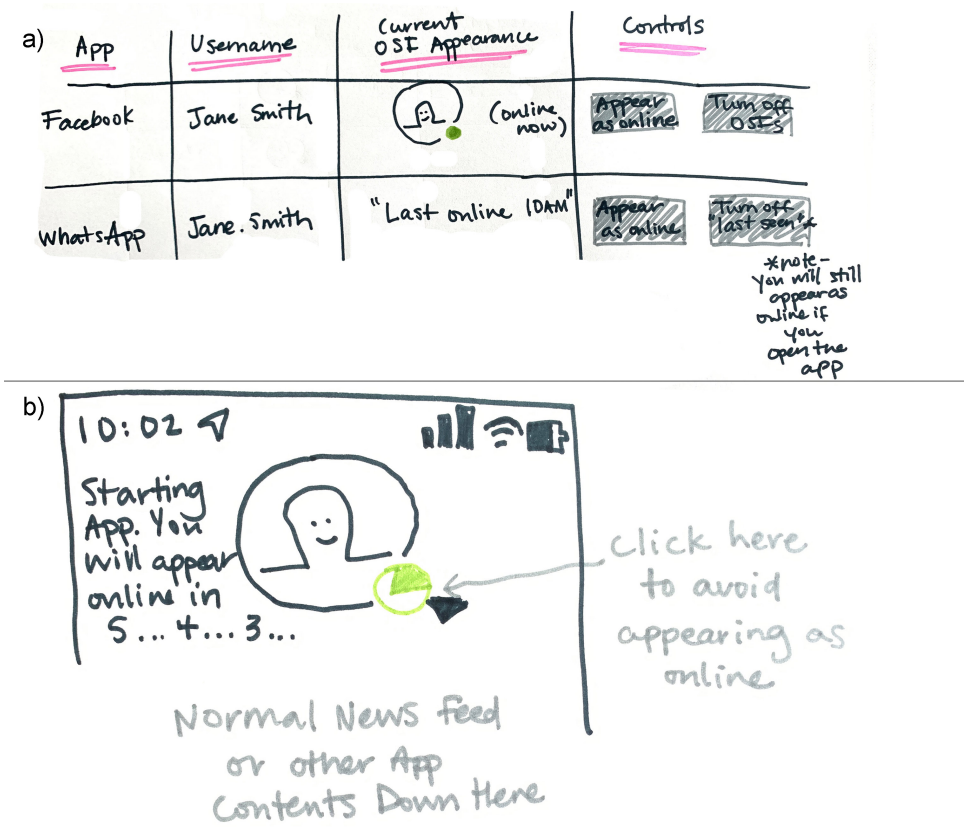


Figure 3.18: Illustrations of design recommendations to create a third-party OSI manager tool (a) and let users turn off their OSI as they *open* an app (b)

3.7.3 Design Implications

I found great diversity in existing appearance, scope, default audience, and settings of existing OSIs. Here, I provide guidance for designing OSIs in ways that are consistent with users' mental models and considerate of the concerns users raised in my survey.

- *Green Color Scheme.* The results of my experiment show that using green will better match users' expectations and require less UI support for communicating that a dot is an OSI. Over half of the apps I studied (21) already use green dots to indicate that a user is online. I encourage designers to reuse the pattern of green dots to indicate that a user is online and discourage them from using green dots to convey anything besides online status.

- *Conservative Defaults.* More restrictive defaults for visibility of users' online status can help users avoid OSI-related privacy violations. This echos a recommendation from prior work that presence be made available only to contacts [37]. Further, I recommend that online status be off by default, and that apps actively prompt users to choose whether they prefer to appear online. This would enable users to make an informed, deliberate decision about whether to share their online status.

- *Salient Settings.* Users reported, both spontaneously and when completing the structured task of adjusting their settings, that OSI settings are difficult to find in the apps they use. A few participants said they did not know how or if OSIs could be turned off in the app they were using. Making OSI controls as accessible as possible, for example, by reducing the amount of clicking or scrolling that users must do to change online status settings is likely to better support users in managing their online presentation. If apps have other privacy settings, grouping OSI settings among them is one mechanism for improving discoverability. Of the 10 apps where online status settings are located in menus, almost all of them already adhere to this recommendation.

- *Targeted Visibility.* Users may sometimes prefer to prevent others from seeing that they are online. Designers should include a mechanism to turn off online status. Around half (19) of the apps in my analysis already do this. Further, if it is not detectable whether a user has turned off OSIs or is actually offline, this can provide vital cover for people in abusive relationships whose partner may become angry if they are "hiding" something. Specifically, users may prefer to restrict the visibility of their online status to smaller audiences or individually control which of their friends or contacts can see when they are online.

- *Prominent Placement.* In many apps, OSIs appear in prominent locations such as user profiles, news feeds, or lists of friends, which can increase users' awareness that their own online status is being shared. Less prominent displays might decrease the likelihood of privacy violations due to accidental or casual observation of OSIs. I encourage designers to display online status in prominent location(s) in the app, though I acknowledge the trade-off that this entails.

- *No Reciprocity.* I recommend that apps do not require reciprocal OSI sharing to see someone else's OSI, though I acknowledge the trade-off of whether reciprocity would make users feel obligated to share their online status or whether lack of reciprocity would encourage users to covertly monitor others.

- *Immediate online/offline updates.* I identified that low-level implementation details, such as how long it takes for users to appear as online or offline after opening or closing an app, can affect users' experiences with OSIs. Although short update times create a more fine-grained record of a person's behavior, I believe that it is preferable for OSIs to immediately reflect when someone comes online or goes offline, because this lets users more intuitively anticipate what others will be able to observe. However, especially if an app lacks settings to covertly turn off OSIs, a longer update time may be preferable since it provides plausible deniability as to whether the person was actually online at

any given time.

Although these concrete recommendations follow directly from the empirical findings I report here, there are inherent trade-offs in several of the suggestions I make, specifically my recommendation to display OSIs prominently throughout the app, eliminate reciprocity in OSI sharing, and show updates to users' OSI with high precision. Future research should explore the impacts of these trade-offs, and may lead to novel or contradictory recommendations.

3.7.4 Limitations

I focused on OSI design in mobile applications, but additional nuances may be introduced with browser, desktop, or tablet versions of apps. For example, OSI settings may or may not propagate across devices (*e.g.,* Slack's settings propagate, but Facebook's do not). Browser or desktop apps may expose more information about a user than the mobile app (*e.g.,* Spotify desktop shows friends what a user has been listening to). Apps on different devices may provide different settings (*e.g.,* Facebook provides per-user online status controls on desktop but not on mobile devices). Common practices on computers, such as leaving apps or browser windows open for longer periods of time, differ from those of phone use and may render OSIs less useful for monitoring behavior (or more useful, if the type of device can be inferred).

Apps have many additional features that could act as proxies for online status (*e.g.,* read receipts in iMessage, YouTube watch history that is public by default, and changes to high scores reflected on leaderboards for CandyCrush). These features were beyond the scope of this study, but given that 76 of the 144 apps without OSIs *do* have social features, understanding how closely these features approximate OSIs would significantly expand the scope of research findings that describe privacy implications of online status information.

3.8 Conclusion

In this chapter, I presented a comprehensive design analysis of online status indicators (OSIs) for 40 mobile apps, with particular focus on how the design of OSIs affects users' ability to meet their privacy needs. I also conducted an online survey, finding that users often do not understand how OSIs work and have preferences that are not aligned with current designs. OSIs routinely reveal information that users prefer not to share, and users most often manage this tension by changing their own behavior, because they have insufficient options for changing the interface. Evidence that some users engage in or experience surveillance via OSIs points to the potential for malicious use in interpersonal relationships. I hope that these findings and the recommendations I make in this work will help app designers make more informed decisions about how OSI design affects user experience.

Chapter 4

WOULD YOU RATHER: A METHODOLOGY TO ELICIT REACTIONS TO TECHNOLOGY TRADE-OFFS

Through both my broad study of U2U Privacy in online dating and my focused analysis of OSIs and their impacts on users, I have identified nuanced privacy trade-offs that technology designers and users face. While the methods I have used in my prior work have enabled me to surface these relevant findings, I recognized that a method specifically designed to confront these trade-offs could add value and richness to future studies related to U2U Privacy. In this Chapter, I present Would You Rather (WYR) — a methodology to elucidate users concerns and values related to U2U Privacy trade-offs, generate design ideas, and evaluate design ideas. While there are aspects of this work that are still in progress, I present the aspects of the WYR methodology that are most directly relevant to the research questions presented in my dissertation. The development of this methodology has occurred in collaboration with Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker.

4.1 Introduction

"Would You Rather" is a conversational game played in social settings, often by children and teens [13]. In this game, one player poses a provocative scenario with two options, and the other player(s) must choose between these options. The scenario always starts with the words "Would you rather." Since the game is more conversational than competitive, there is no explicit scoring; however, the "best" scenarios are typically those that result in a split vote or that cause the other player(s) to think especially hard about their choice. Often, the two choices presented are *both* undesirable, for example "Would you rather always be too hot or always be too cold?" Illustrating the pervasiveness of this game in popular culture, there are

many Buzzfeed polls that use the "Would you rather" question format. Some of these polls address technology-related topics and directly informed the early scenarios I created while developing this research methodology [92] (Figure 4.1). I have adapted this game to create a methodology that I refer to as WYR. WYR is a qualitative method can help researchers gain insights into users' views on which technology trade-offs are salient and important to them, and what their choices reveal about their values and preferences. In this chapter, I will discuss other methodological work that informs the development of WYR, describe the basic WYR methodology and its adaptations such that it can be used to contribute specific types of research insights, and describe preliminary findings from two WYR deployments focused on OSIs. I conclude with a discussion of planned future work to understand how WYR can be applied even more broadly than I have done for my dissertation and the types of insights and research contributions that WYR can offer.

4.2 Related Work

4.2.1 Ipsative Measures

Forced Choice Surveys or Questionnaires, which use "ipsative" measures, in which respondents must choose their preferred option between two choices have been studied and used extensively in psychology [5, 11], and have made their way to marketing research as well [50]. These types of questionnaires and surveys have many similarities with the game Would You Rather, and the extensive quantitative understanding of how they reflect participant preferences will be particularly relevant to my planned future work of adapting WYR to suit quantitative analysis. However, three key differences between these surveys and the current design of the WYR methodology are (1) the intended provocativeness of questions in WYR compared to the relative banality of those used in psychology and marketing, (2) in WYR, scenarios are typically voted on *and* generated by participants, and (3) WYR is designed to work in a public or collaborative setting in which participants' choices and scenario generation are influenced by their conversations and, thus, the dialogue and discussion throughout

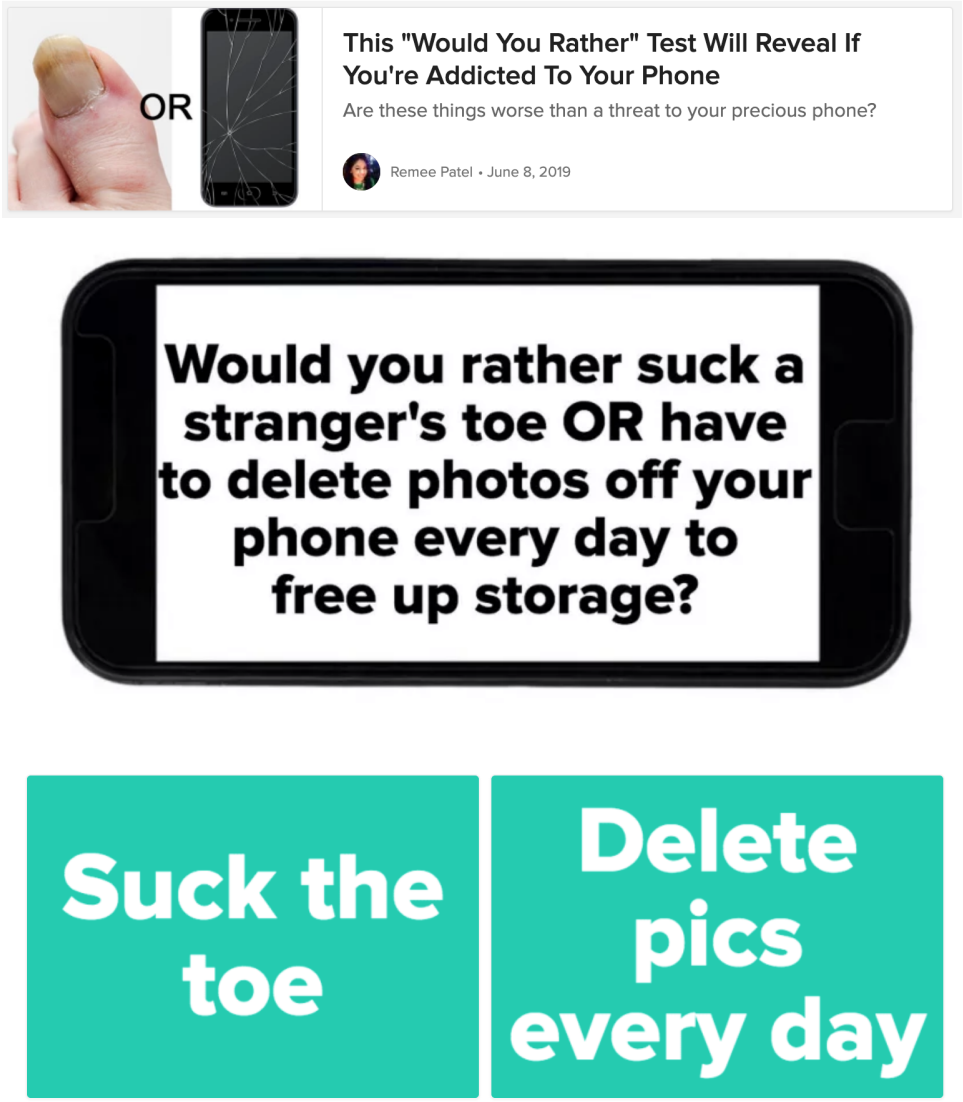


Figure 4.1: The thumbnail image and one question from a Would You Rather poll on Buzzfeed that focused on topics related to technology use.

the activity provides as much of the research contribution as the votes themselves. Within the realm of computer science, one specific type of provocative forced-choice question — the trolley problem — has been used to understand peoples' ethical decision-making preferences and how they should apply in the context of autonomous vehicles [58, 87].

4.2.2 Developing Design Methods

WYR is far from the first method that seeks to learn from users in order to inform better technology designs. For example, comicboarding scaffolds the brainstorming process by providing participants with a partially incomplete comic strip, and is especially useful for brainstorming with children [88]. Similarly, DesignLibs builds on the creativity of MadLibs games by presenting fill-in-the-blank or question-and-answer structured design scenarios to encourage participants to generate more creative, diverse, useful, and/or feasible design ideas [30]. One key property of WYR is that it encourages participants to consider scenarios in which they imagine a version of the world that is not bound to the constraints of reality. Similarly, an existing method called Fictional Inquiry found that situating collaborative design activities in imaginary contexts (*e.g.,* on Mars) led participants to think more creatively, which is beneficial to design processes [51]. Most of these design methods, including WYR, leverage scenarios as a key component of the design process. Five key benefits of scenario-based design were described in 1999 by Carroll, for example, that scenarios are "at once concrete and flexible" [39].

Another key property of WYR is that it provides opportunities for participants to discuss their views with each other and with researchers. Many prior studies have shown and/or leveraged the value of incorporating participants in design activities in collaborative ways [99]. Compared to other collaborative design activities, the public voting aspect of WYR presents a unique limitation in terms of analyzing votes. Because of the impacts of social conformity [83], participants' votes may not actually represent the way they would vote independently.

4.2.3 Privacy Paradox

Prior work has shown that participants' statements about their privacy intentions may not match their actual behaviors. The phenomenon of users who report wanting privacy but not acting in privacy-preserving ways is referred to as the Privacy Paradox [71, 90]. Much of the work presented in this dissertation demonstrates that users actually hold very nuanced views and preferences related to how they present themselves online, which may not be sufficiently demonstrated through their privacy-related behaviors. Since WYR scenarios are designed to present approximately "even" trade-offs, participants' votes on these scenarios may represent a preference that more closely matches the behavior they would exhibit if they were actually faced with that scenario. It is beyond the scope of my dissertation to explore the circumstances in which participants' WYR responses are or are not examples of the Privacy Paradox; however, the WYR method is not intended to primarily focus on which option(s) an individual chooses but rather to more broadly prompt and inform discussion about technology design and the tensions and trade-offs users encounter.

4.3 WYR Core Method

The basic structure of a WYR deployment includes 3 parts: (1) scenario generation and selection, (2) voting, and (3) discussion and analysis (Figure 4.2). Each of these parts can be conducted independently (*i.e.,* it is not necessary to include all three parts in every WYR deployment) and/or could happen synchronously with another part(s), and each part can be modified such that the WYR deployment suits a certain context or to achieve a certain set of research outcomes. In this section, I will describe each part of a WYR deployment and the possible ways to structure that part of the deployment to fit the context and goals of the deployment.

At a high level, there are two main contexts in which it may be appropriate to deploy WYR: (1) focus group-style activities, in which there is an opportunity to fully describe the relevant research questions and create structured settings for brainstorming and discussion,

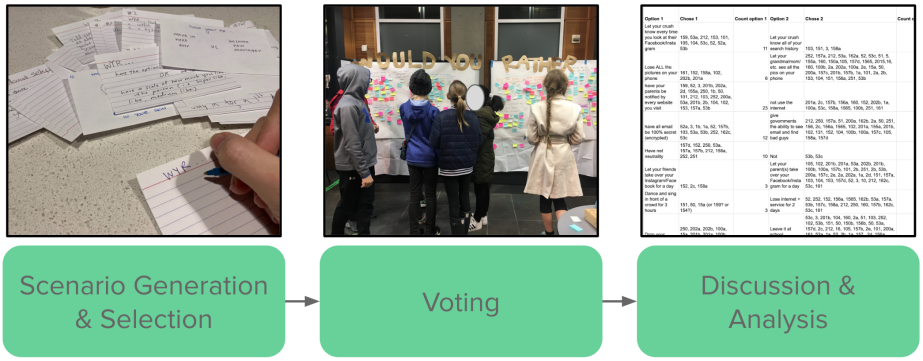


Figure 4.2: The basic structure of a WYR activity consists of three parts: scenario generation and selection, voting, and discussion and analysis.

and (2) open house-style activities, in which participants engage with the activity for varying amounts of time and depth and may or may not engage directly with researchers. A third context in which WYR deployments may be appropriate is online; however, I have not yet deployed WYR in this way an present only plans for future online deployments. In this section, I provide examples of how an online context could impact a deployment, but I focus mainly on in-person deployments.

I have identified three key potential contributions of a WYR activity: (1) elucidate users concerns and values related to U2U Privacy trade-offs, (2) generate design ideas, and (3) evaluate design ideas. All three of these contributions can be made through qualitative analysis of WYR data, contingent on certain aspects of how the deployment was conducted. I highlight WYR deployment changes that could enable quantitative analysis, though I have yet not prioritized this aspect of WYR in previous deployments.

4.3.1 Scenario Generation and Selection

The first step in a WYR activity involves generating WYR scenarios and then, optionally, narrowing the generated scenarios down to a smaller set for voting. Scenarios can be gener-

ated and/or selected by researchers, participants, or a mix of both.

Participant-Generated Scenarios

Participant-generated scenarios offer insight into what users value and what tensions are salient to them, for example, based on the themes that emerge across scenarios. However, I found that it can be difficult for participants to create high quality WYR scenarios. Participant-generated scenarios sometimes deviate from the intended thematic focus of an activity, are poorly balanced, and/or present a trade-off where it is unclear how each side of the scenario relates to the other. I have developed several suggestions for improving the quality of participant-generated scenarios:

- Provide opportunities for participants to brainstorm scenarios in groups.

- Include researcher-generated "seed" scenarios (*i.e.,* do not start with an empty wall where participants are meant to add their own scenarios). Seed scenarios can help convey a thematic focus of the activity in contexts where there may not be a chance to verbally convey the goals of the activity to every participant. Researcher-generated seed scenarios can also provide examples to demonstrate how each half of a scenario might be related to the other.

- Separate scenario generation from scenario selection. Although this may not be practical in all contexts, I found that the chosen scenarios were of higher quality when participants were encouraged to write generate more ideas and then pick the best ones.

- Involve researchers in scenario brainstorming. For example, in one deployment of WYR, a young participant deviated from the intended focus on technology by suggesting the scenario "WYR freeze to death or burn to death?" A researcher might ask, "How do I bring this scenario back to focus on technology? Is there any technology that controls temperature?" In my deployment, this led to a scenario related to smart thermostats.

- Encourage participants to iterate on existing scenarios. For example, in one deployment participants initially wrote: "WYR go 100 days without Internet or have 100 days where anyone can read your mind?" In this deployment, scenario generation and voting occurred at the same time, and early votes and conversations conveyed that the scenario was not well-balanced (*e.g.,* participants made statements such as "100 days without Internet, obviously. That's easy!"). Researcher guidance may or may not have helped improve the original version of this scenario. However, I found that asking, "What changes could you make to the scenario so that it would become a really hard choice for you?" helped participants modify the scenario to be more balanced. In the previous example, participants suggested modifying the scenario to "WYR go 1000 days without Internet or have 5 days where anyone can read your mind," and subsequent votes were somewhat more balanced (Figure 4.3).

- Provide a source of brainstorming structure or guidance. For example, in one deployment, I wrote examples of partial scenarios, types of technologies, and various stakeholder groups on slips of paper that participants could pull from a box.

Researcher-Generated or Researcher-Selected Scenarios

When scenarios are generated by researchers, the WYR deployment will almost certainly lead to a very different type of research contribution. Most notably, removing participant-generated scenarios removes the possibility of analyzing themes that occur across scenarios to understand what the scenarios themselves reveal about user tensions and preferences.

While my work thus far has predominantly focused on the possibilities of participant-generated scenarios, researcher-generated scenarios can have important advantages as well. In particular, researchers may be in a better position to generate higher quality scenarios or scenarios that focus on trade-offs related to their specific research questions. Researcher-generated scenarios may be inspired by previous research findings, design recommendations, or participant-generated WYR scenarios from past deployments. The following list of WYR

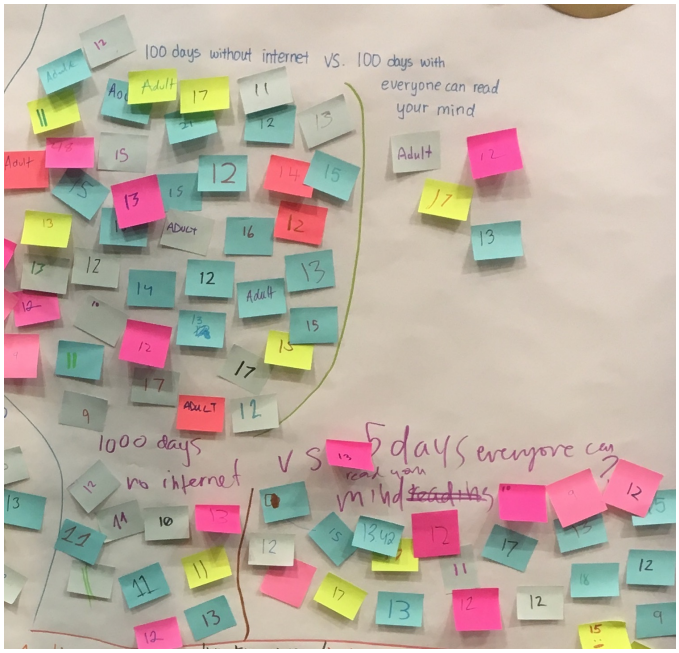


Figure 4.3: In a typical WYR deployment, scenarios are written on a whiteboard or large piece of paper taped to a wall. Sticky notes are used to cast votes and may have something written on them, such as demographic information about the person who cast the vote. The two scenarios shown here demonstrate how encouraging participants to iterate on scenarios can help them find more balanced trade-offs.

scenario formulations is a synthesis of participant-generated scenarios and participants' commentary on popular WYR scenario formulations.

Example Formulations of WYR Scenarios

I have found that knowledge of common structures of WYR scenarios is useful for researchers generating scenarios or guiding participants toward better scenarios. The following list of WYR scenario structures and concrete examples is a useful starting point but is not intended to be exhaustive.

- **Always or Never.** *WYR Always appear as "online" or never appear as "online"?*

- **Extreme Opposites.** *WYR your smart thermostat malfunctions and sets the temperature in your home to -10 degrees in the winter or 100 degrees in the summer?*

- **Varying the stakeholder.** *WYR your parents see all of the photos on your phone or your colleagues and boss see all the photos on your phone?*

- **Data Loss or Data Compromise.** *WYR your parents see all the photos on your phone or all of the photos on your phone are deleted forever?*

- **Varying the asset (*e.g.*, type data) that is impacted.** WYR your parents see all the photos on your phone or all of your Internet browsing and search history?

- **Altering the likelihood, frequency, or length of impact.** *WYR 100 days without Internet or 100 days when anyone can read your mind? WYR have to re-type your password every time you look at your phone or have to authenticate with a finger prick of blood once per day every day? WYR your partner sees a really mean breakup text you sent but no longer mean or risk the possibility of getting caught sneaking into their phone to delete it?*

- **A but B or A' but B'.** *WYR find the love of your life tomorrow but also have a stalker or take 10 years to find the love of your life but everyone you meet in the meantime is kind to you?*

4.3.2 Voting

Voting is the only component of a WYR activity that *necessitates* participant involvement. Researchers can derive qualitative and/or quantitative research contributions from voting depending on how the voting is structured. So far, my WYR deployments have predominantly focused on collecting data for qualitative analysis, though these are not mutually exclusive possibilities.

The basic voting process for in-person deployments involves placing sticky notes on whiteboards or large pieces of paper where scenarios have been written, as shown in Figure 4.3. I found that this visual representation and the in-person, synchronous, non-secret aspects of voting helped facilitate conversations between participants and between participants and researchers. In Section 4.3.3, I will describe how researchers can take advantage of these conversations for qualitative analysis. However, I have also identified several adaptations in terms of *how* the vote itself is structured that can contribute to these discussions or can enable more meaningful *quantitative* analysis:

- **Annotated Voting.** Ask participants to write demographic information on sticky notes or to encode demographic information in the color of sticky notes they use. For example, in one deployment, participants' votes included their age. Noticing that an adult had voted the same way she had, an 11-year-old participant thought aloud to a researcher: "Why would an *adult* prefer ...?" This led to a discussion about how adults' and kids' security and privacy practices compare; this conversation would likely not have been occurred without demographic information being displayed on each vote. Participants may notice patterns that are not necessarily statistically meaningful but can nevertheless help us learn more about their understanding of the world.

- **Alternate-Perspective Voting.** Ask participants to cast votes *as though* they were an adversary or another type of stakeholder (using a different color of sticky note). For example, after participants have cast their own vote, one can ask them to vote the way they believe their parent, child, partner, or boss would vote, or the way they think an abusive partner, an oppressive dictator, or another type of adversary would vote. Most of the WYR scenarios I present are phrased such that the choice will only impact the person voting. When asking participants to vote as though they were an adversary, I found it was important to rephrase the scenarios using a formulation such as "WYR a world in which people do X or a world in which people do Y?" This way it is clear that participants are answering "Which of these options would be easier for an adversary to take advantage of?" rather than "Which of these options would make it harder for an adversary to get caught being adversarial?" or some other ambiguous interpretation.

- **Voting with Attribution.** Track individual participants' votes. For example, in some of my deployments, I assigned ID numbers for participants to write on their sticky notes. Although I find that this adds substantial overhead in terms of researcher involvement, it is necessary for certain types of quantitative analysis such as observing whether there are patterns in how specific users vote across all questions.

- **Reducing Bias in Votes.** Take steps to minimize the impact of other votes/voters. I recognize that because participants can see previous votes in the basic implementation of a WYR activity, an early skew in voting may influence their choices (*i.e.,* exhibiting social conformity [83]). When participants vote while being observed by friends, family or other participants, this may also affect how they vote. Although I have not yet explored these possibilities in my deployments, researchers could obscure or intentionally manipulate previous votes, or isolate voters. I believe these changes and experiments are most well-suited to online deployments.

4.3.3 Discussion and Analysis

Discussion is one of the most fruitful aspects of a WYR deployment in terms of its contribution to a qualitative, nuanced understanding of participants' views on the trade-offs presented through WYR scenarios. For the most part, I find that standard best practices for research that involve interviews is sufficient in WYR discussions. However, since interviews generally involve just one participant at a time, I find that it is especially important at a WYR deployment to ensure that enough researchers are present (but not too many). The number of researchers present, particularly for WYR activities that occur in relatively public settings, needs careful balance. Too many researchers can make participants feel intimidated and avoid even casting a vote. During the OSI-focused deployment, I found that even one researcher in close proximity to the voting area detracted from participant engagement. Without enough researchers present, however, I have felt that I was unable to sufficiently capture the interesting aspects of participants' conversations with us or with each other. Audio or video recording devices can help with some aspects of this, albeit at the expense of increased setup costs and added potential for participants to hesitate to become involved.

Some guiding questions that I find useful to engage participants in discussions include:

- Are there any scenarios that you found especially difficult or easy to decide about?
- Are there any vote outcomes that surprise you?
- Are there any scenarios that you thought were especially funny or creative?
- How did you make your decision about [specific scenario]?
- How would we have to alter this scenario to get you to choose the other option?
- Do you know anyone who you think would choose differently than you did for [specific scenario]?

- Why do you think someone might choose the other option for [specific scenario]?
- How would your redesign [specific technology] based on this activity?

The analysis I have done thus far regarding WYR data (*i.e.,* generated scenarios, selected scenarios, votes, and participant discussions) has involved identifying themes in terms of what this data reveals is salient, important, or preferable to participants. Researchers' follow-up discussions could focus on how these values might lead to new technology design ideas or recommendations.

Although I have not explored quantitative analysis of WYR votes, I am excited about the possibilities of doing so in future work, particularly in our planned online deployments. For WYR deployments with a sufficient number of participants, quantitative analysis might allow us to evaluate novel design ideas or existing design patterns in a statistically meaningful way.

4.4 Iterative Development of the WYR Core Method

Over the course of approximately two years and a half years, I have deployed WYR seven times in a variety of contexts. Throughout the course of this work, I have maintained an iterative process journal, and in each subsequent deployment, I have introduced strategic changes to better understand the benefits and limitations of WYR. Chronologically, these seven deployments include:

1. *Probing Children and Parents' General Security Concerns at an Open House Event (1)* — First deployment of WYR, in which participants (children and their parents) were assigned ID numbers and voted on a mix of researcher-generated seed scenarios and participant-generated scenarios broadly themed around technology in general.

2. *Probing Researchers' General Security Concerns at a Happy Hour Event* — Although we anticipated that the main difference between this and the initial deployment would be the age and level of tech expertise of participants, we observed that the more

stagnant nature of participants' movement through space at this event resulted in fewer votes and made it more difficult for researchers to engage in conversations about the scenarios with participants. Like the first deployment, we assigned participant ID numbers and participants voted on a mix of researcher-generated seed scenarios and participant-generated scenarios broadly themed around technology in general. Another key difference is that this deployment took place during a recurring weekly event where attendees expect to casually "compete" and for organizers to choose a winner. Thus, participants were incentivized to contribute scenarios by the promise that the "best" scenario would win.

3. *Probing Children and Parents' General Security Concerns at an Open House Event (2)* — The demographics, broad focus on technology, and mix of researcher- and participant-generated scenarios in this deployment were consistent with the initial deployment. During this deployment, I paid special attention to the strategies I used to encourage participants to contribute their own scenarios, to help participants generate on-topic scenarios, and to engage participants in conversation about their preferences. With this in mind, I introduced a box from which participants could draw partial scenario ideas, types of technologies, and stakeholders who participants might care about keeping things private from.

4. *Introducing WYR to Students Considering Security Course Project Ideas* — This deployment was the first time we did not provide any researcher-generated scenarios, the first time the WYR scenario generation, voting, and discussion would occur sequentially rather than synchronously, and the first time we could anticipate the number of participants and expect a relatively small group discussion, since it occurred in a classroom setting. Participants were expected to arrive with an idea for their capstone project, and they worked with a classmate to brainstorm how those ideas could suggest a WYR scenario. Thus, these were also the first scenarios which were generated with a *specific* technology question in mind (albeit not by the researchers).

5. *Using WYR as an Introduction to Security and Privacy in a Computer Science Course for Non-Majors* — In this deployment, I sought to understand whether WYR was viable as an educational tool. The educational aspect of that deployment is outside of the scope of my dissertation work; however, this deployment is the only deployment so far where we have asked participants to first vote with their own preference and then to use another colored sticky note to vote "as though they were an adversary."

6. *Seeking Researchers' Preferences to WYR Scenarios Focused on OSIs* — This deployment is the only deployment where all scenarios have been researcher-generated. It is also the first deployment in which the scenarios were intended to address a specific topic — OSIs. This deployment is described in greater detail in Section 4.5.

7. *Exploring Tensions and Values Related to Online Dating in a Graduate-Level Class on Technology Design* — This deployment included only participant-generated scenarios. It included an even more structured scenario-generation process that encouraged participants to generate more scenarios than they would ultimately vote on. This deployment is the only deployment that has had participant-generated scenarios focused on a researcher-specified topic — Online Dating. This deployment is described in greater detail in Section 4.5.

In addition to the deployments enumerated above, we invited researchers and students in project-based, design-focused courses to utilize the WYR methodology. We first offered this methodology to students in the capstone course based on guidance that was written by Lucy Simko shortly before the 4th deployment and also utilizing the deployment described above, which those students participated in, as an example. Next, we described WYR to another researcher around the time of the 6th deployment. Finally, the 7th deployment was used as an example along with a short verbal description of possible adaptations to convey the methodology to another group of students. Although I have received IRB approval to request students' coursework which utilized the WYR methodology, incorporating others'

results, experiences, and general feedback from deploying WYR was outside of the scope of my dissertation. I have not yet requested this coursework and can, therefore, not comment on whether any students actually chose to use WYR; however, the exercise of distilling what we learned from our deployments such that we could describe WYR to other researchers was an important aspect of the development of this methodology.

After all of these deployments, the research team conducted a secondary analysis of data from our deployments, which included the participant-generated scenarios, votes on all scenarios, and notes from our iterative process journal. The outcome this work is the Core WYR Method described previously.

4.5 Case Studies

In this section, I present two case studies of WYR deployments. These case studies demonstrate both primary contexts in which WYR could be deployed, show both more successful and less successful participant engagement, and demonstrate how WYR can be adapted to focus on specific research questions or goals. I present these case studies chronologically in terms of when each deployment took place.

4.5.1 WYR Deployment Focused on OSIs

My sixth deployment of WYR focused on the topic of OSIs. This deployment took place during a student research poster session for the UW iSchool; I presented a poster and considered the WYR deployment as a "research demo." While the poster session was well-attended, the four scenarios that participants voted on received a combined total of only 66 votes (between 14 and 18 votes per scenario).

I generated and selected four scenarios in advance, because I anticipated that the physical space for voting would be much more limited than a typical deployment and because I found that it was difficult to think of creative WYR scenarios related to OSIs. The four WYR scenarios and voting outcomes are shown in Figure 4.4. These scenarios were chosen to highlight themes, trade-offs, or stories identified in my previously described research on OSIs

(Chapter 3). For example, scenario 1 brings up the tension that participants expressed related to feeling a sense of obligation to reply right away if others can see that they are online, compared to the potential loss of convenience and reliability of modern messaging technologies. Scenarios 2 and 3 draw on the themes from my work on OSIs that many participants conveyed stories in which their experiences with OSIs involved their (former) romantic partners or people they work with. In scenario 4, I imagined an exaggerated version of OSIs, in which other people could either see a video of the user or the user's screen; I hoped that this would prompt participants to think more imaginatively about what someone would be able to learn about their behavior when they are online.

The actual voting and discussion outcomes of this deployment were not particularly insightful. I found that participants at this event were more eager to engage with the activity when I was not nearby, and, thus, I was not able to have conversations with many participants. Because the event was primarily a poster session conveying research results, most people who spoke with me wanted to learn more about the project at a high level rather than discussing the scenarios. I also observed that people seemed interested in the scenarios and may have discussed them with friends or colleagues even if they did not actually cast a vote. One participant placed their sticky note in between the two options for scenario 4 and wrote "No," showing that they were not willing to accept either option in this scenario. Even without having a conversation with this participant, the way that they participated demonstrates the potential for participants to shape the activity to highlight their values and preferences and to inject elements of playfulness and self-expression.

Despite these limitations, this deployment had several positive outcomes. Since this was the first deployment in which I aimed to focus on a specific topic, the exercise of generating WYR scenarios provided the insight that some structure would be necessary in order to ask participants to generate scenarios focused on a specific topic. This insight informed my planning for the next deployment, which I discuss as a case study in Section 4.5.2. In addition to letting my prior work on OSIs inform my scenario generation, I found that having examples of types of "good" WYR scenarios was helpful, and this led me to conduct

additional analysis of many scenarios to distill them to the list of "Example Formulations of WYR Scenarios" at the end of Section 4.3.1.

4.5.2 WYR Deployment Focused on Online Dating

I had three main goals for my most recent deployment of WYR had three main goals: (1) further iterate on previous experiences in focus group-style deployments, (2) focus on online dating, and (3) focus on scenario generation, not just voting, by encouraging participants to brainstorm more scenarios than in previous deployments. This deployment took place in a classroom setting — a graduate-level class of approximately 30 to 40 students focused on technology design. A total of 47 scenarios were generated; of those, 11 Scenarios were voted on and received between 12 and 24 votes each, for a total of 215 votes.

First, participants formed 11 groups. I provided each group with a short set of instructions (Figure 4.5) including an assigned "phase" in online dating and an example of how they could use that phase to think of relevant WYR scenarios. Participants spent about 10 minutes brainstorming scenarios, writing each one on an index card. Once they had written several scenarios, each group swapped index cards with another group and chose their favorite scenario that the other group had come up with to write on the board for voting.

Since this deployment also served as an example of how to deploy WYR, such that the students could use it in their course projects, I gave participants choices about how to conduct voting. I provided three colors of sticky notes, and they decided to use sticky note color to convey their gender — blue for women, pink for men, and green for non-binary people, though everyone chose to vote with pink or blue. No one commented on any gendered patterns in votes during our discussion. The 11 selected scenarios and final votes are shown in Figure 4.6. Scenario selection and voting lasted around 25 minutes.

Discussion during this deployment was fruitful. I encouraged participants to focus on three discussion topics: (1) how to do WYR in other contexts, (2) what makes a "good" WYR scenario, and (3) what we could learn from the scenarios they generated and votes they cast. Several key themes that were present in my prior work related to online dating re-emerged in

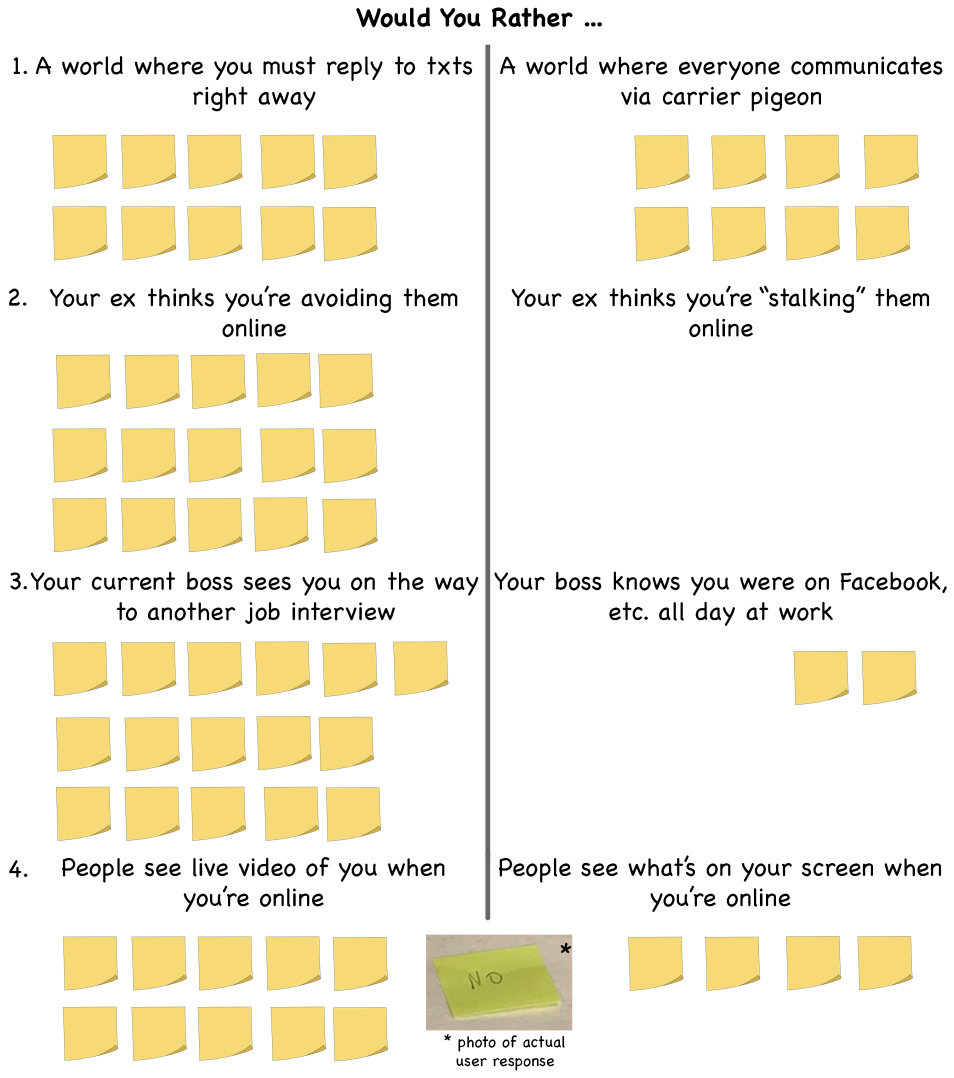
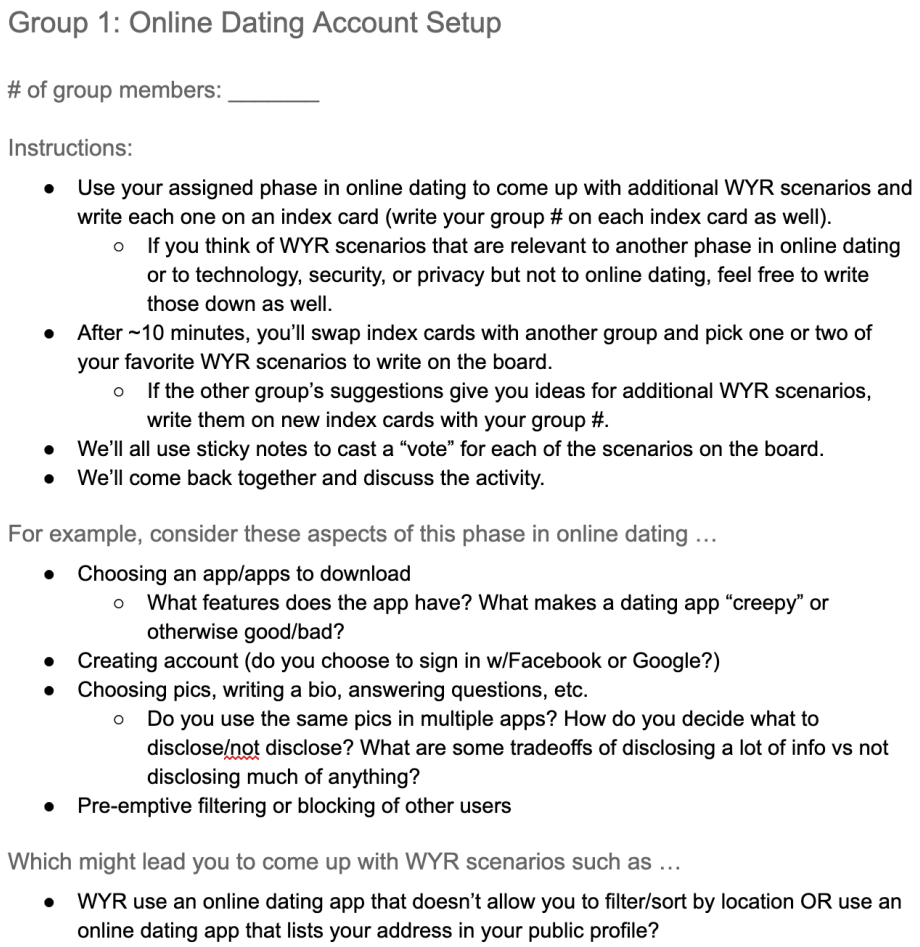


Figure 4.4: Four researcher-generated WYR scenarios and participant votes focused on OSIs.



Group 1: Online Dating Account Setup

# of group members: _____

Instructions:

- Use your assigned phase in online dating to come up with additional WYR scenarios and write each one on an index card (write your group # on each index card as well).
  - If you think of WYR scenarios that are relevant to another phase in online dating or to technology, security, or privacy but not to online dating, feel free to write those down as well.
- After ~10 minutes, you'll swap index cards with another group and pick one or two of your favorite WYR scenarios to write on the board.
  - If the other group's suggestions give you ideas for additional WYR scenarios, write them on new index cards with your group #.
- We'll all use sticky notes to cast a "vote" for each of the scenarios on the board.
- We'll come back together and discuss the activity.

For example, consider these aspects of this phase in online dating …

- Choosing an app/apps to download
  - What features does the app have? What makes a dating app "creepy" or otherwise good/bad?
- Creating account (do you choose to sign in w/Facebook or Google?)
- Choosing pics, writing a bio, answering questions, etc.
  - Do you use the same pics in multiple apps? How do you decide what to disclose/not disclose? What are some tradeoffs of disclosing a lot of info vs not disclosing much of anything?
- Pre-emptive filtering or blocking of other users

Which might lead you to come up with WYR scenarios such as …

- WYR use an online dating app that doesn't allow you to filter/sort by location OR use an online dating app that lists your address in your public profile?

Figure 4.5: A short set of instructions were given to each group in my online dating-focused WYR deployment. Each group was assigned one of five "phases" in online dating (account setup, viewing others' profiles and conversing in-app, setting up and going on early dates, longer term dating, and breakups or "ghosting") and given some example WYR scenarios pertaining to that phase, which were informed by my previous research in online dating.

	Option 1	Votes - women	Votes - men	Option 2	Votes - women	Votes - men
1	Go on a blind date	3	1	**Go on a date with an acquaintance**	11	4
2	**Ghost the love of your life**	9	5	Have the love of your life ghost you	4	2
3	**Get ghosted and have them see you on a date with someone hotter**	7	5	Review their application for a job at your company	6	2
4	**Have the option to just "like" a profile**	10	4	Have a scale of how much you like them (superlike, medium like)	2	5
5	**You just broke up. Have your ex move in next door**	6	6	Have your ex become your new manager	0	0
6	Admit that you've been dating your significant other long term because you guys met through being catfished by them	1	0	**You met through drunkenly booty calling them 3 seconds after matching at 3am**	10	5
7	**Have your date lie about their income**	13	4	Have your date lie about their intentions	3	3
8	Tell people you met your partner on a hookup site	6	1	**Tell people you met your partner on a drunken hookup**	7	6
9	Be required to include a pic of your feet	5	5	**Be required to include a pic of your teeth**	9	5
10	**Meet your date through a mutual friends**	10	7	Have them be a total stranger	4	2
11	Send nudes and they turn out to be a catfish	0	2	**Acidentally send nudes to a legitimate match**	9	6

*Winning option shown in **bold***

Figure 4.6: Participants chose to vote on this subset of 11 scenarios out of a total of 47 participant-scenarios generated on the topic of online dating. Given the suggestion that sticky note color could be used to denote some personal characteristic, participants collectively decided to use the color of sticky notes indicate their gender.

this deployment: concerns about overlap between online dating experiences and employers or coworkers, concerns about information disclosure and what users feel comfortable revealing in profiles (or not), also addressing what they want to see in *other users'* profiles.

Through group discussion and subsequent analysis of these results, we have identified several ways that the results of this deployment might inform design choices for online dating services. Scenarios 1 and 10 both address the trade-off between meeting a potential date who is a stranger versus meeting through mutual friends or as a set-up. In both cases, participants preferred to meet through mutual friends. This preference is already reflected in dating apps in some ways — some dating apps already have features that allow users to know if they share mutual friends or that intentionally prioritize matches between people who have mutual friends (*e.g.,* Tinder used to show mutual Facebook friends, and the entire initial premise of Hinge was to make matches via existing connections). Tinder also included a feature that let users play matchmaker for their friends [72]. Perhaps users would prefer more of these features, or versions of them that address other tensions and trade-offs that may arise if those features gain popularity: Do users *actually* want all of their friends to pair up around them? How would the matchmaking user feel when their friends did not like each other? Or if they hit it off for a while and then had a complicated break-up?

As in my previous work, the theme of tensions related to accidentally encountering employers and coworkers came up in this deployment. The decisive vote on scenario 5 shows that people would not want their ex to be their boss, and the theme of employment decisions is also present in scenario 3. I am only aware of one online dating app that has built-in functionality to help users avoid their coworkers — The League does so by asking users to connect their LinkedIn account, but rather than highlighting this feature, The League pitches itself as an "exclusive" dating app for people who are especially smart, interesting, or wealthy, which may not appeal to all users who care about avoiding their coworkers [66].

Scenario 11 demonstrates a tension related to accidentally sending sensitive content (nude photos), and several other scenarios also address examples of photo sharing that might make users uncomfortable (*e.g.,* scenario 9 and several scenarios that were not chosen to be voted

on). This could lead to design ideation around the goal of helping users prevent (accidentally) using images that might be sensitive, for example by using computer vision to detect nudity and confirming that users *actually* want to send questionable images.

Other scenarios, including scenarios 6, 7, and 11 demonstrate participants' concerns about the honesty of people they meet via online dating (note that "catfishing" involves creating a fake or misleading online persona to attract or trick matches). The online dating service Bumble has adopted a "photo verification" feature aimed to help prevent catfishing [16], but other aspects of matches' honesty such as their income or intentions (scenario 7) cannot be addressed through photo verification. Enabling participants to demonstrate their trustworthiness without compromising their privacy preferences is a promising direction for future design work in this space.

Overall, this deployment was an example of how scenario generation can be adapted to concentrate on a specific topic and produce more scenarios. I have illustrated how themes in the data (participant-generated scenarios, final voting outcomes, and my notes about the discussion) could lead to productive design ideas. Although both of the design suggestions I bring up have some precedent in existing dating apps, this does not negate the fact that these ideas arose from an independent approach, and I have discussed how follow-p WYR scenarios could be used to further understand what types of potential designs users would prefer.

4.6 Discussion and Conclusion

In this chapter, I have presented a methodology called "Would You Rather" (WYR) in which participants or researchers create provocative forced-choice scenarios, and participants vote on those scenarios. WYR can be used to generate design ideas related to specific technologies or aspects of technologies, and can also help researchers or design practitioners understand users' concerns or preferences related to technology trade-offs. I developed this methodology through seven unique deployments of WYR and analysis of the outcomes and output of each of those deployments. In this chapter, I have detailed two deployments in particular as case

studies for WYR. The case studies I describe are focused on trade-offs related to OSIs and the specific application domain of online dating, both of which I have studied in previous research projects, which are also described in this dissertation. In particular, the case study centered around online dating resurfaced themes that had emerged independently through surveys and interviews in my previous work and led to new ideas for how dating apps could be designed or adjusted to suit certain user preferences. Planned future work related to online dating will explore the potential for WYR to be adapted for use as a quantitative method in addition to offering qualitative insights. For example, online deployments to larger numbers of participants will allow us to explore new variations in terms of the structure of a WYR deployment, see patterns across participants' responses to multiple scenarios or in terms of how different demographics of users react to certain scenarios, and avoid certain types of bias such as the effects of social conformity that might affect how participants vote.

Chapter 5
CONCLUSIONS

In this chapter, I reflect on the themes and findings that this dissertation has surfaced related to U2U Privacy in social and communications apps. I then share directions for future work in this domain. Finally, I conclude with final words.

5.1 Themes and Reflections

In my dissertation, I have identified several themes that carry through the work I have conducted. Many of these themes lead to broad recommendations for design that are applicable beyond the specific context of online dating or OSIs; other themes can act as useful starting points for researchers or designers seeking to understand U2U Privacy considerations related to other common app features or app genres or in emerging technologies beyond those I have studied in this dissertation. In this section, I will relate these themes back to my two original overarching research questions, posed in Chapter 1.

5.1.1 Practices and Preferences Related to Information Disclosure

Disclosure Preferences Depend on Audience

Participants in the studies I have conducted expressed diverse preferences in terms of what they were willing to share with people they knew, including employers, coworkers or colleagues, romantic partners or former romantic partners, and family members, especially their parents. In some cases, particularly in the context of online dating, their sharing preferences were *more* restrictive for people they knew than for strangers. However, participants also described situations or types of data for which they found it useful or fulfilling to share personal data with certain people. For example, some participants felt that seeing people

they knew using online dating created a sense of togehterness stating that it was "kind of nice to know we're all in the same boat." Because users' sharing preferences in terms of audience are so nuanced, a key design implication is that apps should be designed such that users can control how they present themselves to specific other users. The balance of providing features that give users such fine-grained control without overwhelming them with settings options is non-trivial, but a potentially useful guiding principle for achieving this outcome, which I recommended in Chapter 3, is for apps to provide more restrictive default settings for the audience of their personal information and enable users to select who should have access to their information.

Disclosure Preferences Depend on Situational Factors

Though it is far from a novel insight, I found that users are sometimes willing and sometimes not willing to disclose certain information about themselves (*i.e.,* they were able to describe situations they had actually experienced in which they had wanted to disclose or not wanted to disclose certain information). For example, some participants expressed a desire to be able to appear as offline so that others would not distract them while they were trying to get work done, or if they were only planning to come online for a brief time but not intending to start a conversation. Designers should make it easy for users to determine whether to disclose information such as their online status at any given time and to later change their mind about this choice to disclose that information.

Implications of Disclosure Depend on Personal Characteristics

One key finding of my analysis of Tinder profiles is that people with particularly unique names were more likely to be identifiable based on the information in their profiles. This finding was echoed as a concern by participants in my surveys and interviews — for people with unique first names, apps that require them to share this seemingly mundane information disproportionately impede their ability to be anonymous compared to other users, regardless of what other information they choose to disclose. This finding has implications that are much

more broad than disclosure of first names in online dating profiles — the same information may present a greater risk or sensitivity for some users than others, depending on their personal characteristics or circumstances. For example, OSIs may present a much greater risk to people experiencing domestic violence. While I would encourage app designers to consider and design for particularly obvious, common, or severe U2U Privacy risks that affect only some users, a more general design principle is to provide options such that users can understand and control their self-presentation to suit their own needs.

5.1.2 How Design Influences Disclosure

Throughout my dissertation, I have repeatedly found ways that design influences what users (choose to) disclose to other users. In the same sense that technical security and privacy is (or should be) built into technology from its beginnings, designers should devote substantial effort to understanding what, how, when, and with whom users might want to share information about themselves (or not).

Misunderstandings About App Features Lead to Unintentional or Unconscious Disclosure

I have found that misunderstandings can lead users to unintentionally or unknowingly broadcast certain information about themselves to other users. These misunderstandings can include to not realizing that taking certain actions will cause information to be broadcast (*e.g.,* not realizing that opening an app will cause them to appear as online), because their understanding of a similar feature in another app does not apply to all apps, or because they are unable to anticipate how other users will behave in an app.

Designers should find ways to make it clear what information about a user has been and/or will be broadcast, and provide ways to prevent broadcasting certain information *before* it happens. For example, when users create a new account in an app that has OSIs (*e.g.,* OKCupid), their online status will be broadcast as soon as they have set up the account, even before they realize that this information is being broadcast and before they have a chance to change OSI privacy settings (if settings exist). On Tinder (at the time

of my study of online dating), users' profiles were automatically populated with pictures, educational history, and employment information directly from Facebook, and the profile was immediately shown to other users, even before the user had a chance to curate their own profile. In my own personal experience, this once meant that my Tinder profile briefly included a newspaper photo of me as a child with my dad, including a caption that revealed my hometown and my full name. This was not information that I would have chosen to share so publicly, but several other users noticed and commented on the picture before I had a chance to update my profile. Tinder could have prevented this accidental disclosure through the design of their app by not showing users' profiles until they specify that they are finished setting it up.

Users should also be able to transparently understand what information has been broadcast about them previously. For example, at any given time, a user's online status may not be particularly meaningful; however, patterns in online status over time can leak more sensitive information. A user should be able to incorporate their understanding of what they have previously broadcast about themselves into their sharing decisions in the present and future.

Designers should provide a consistent user experience with how their behaviors in the app affect their self-presentation. Users should be able to intuitively reason about how their actions will reflect to other users. For example, in some apps, it may be unintuitive that users appear as online for several minutes or hours after they actually close the app. The functionality of a design feature should be consistent with other apps that have similar features. When social features within an app undergo changes over time, this can result in users' previous understanding of the app being outdated. These changes should be clearly communicated to users.

Users should be able to easily anticipate and control the audience of information they disclose. Based on the findings of my dissertation and prior work, it is clear that users may have different sharing preferences for different people at various times. For example, many participants in my survey related to OSIs described times that they preferred not to be seen

as online by certain friends because of a specific interpersonal circumstance; however, most current OSI designs are not supportive of users who wish to selectively hide their OSIs at certain times or from specific other users. In my interviews and surveys related to online dating, many participants described instances in which they were surprised to see someone's profile or surprised to realize that their profile had been seen by certain other users — they found it difficult to anticipate the audience of their profile, which meant that they could not necessarily make informed choices about what they preferred to disclose.

5.1.3 Design Can Coerce Users to Disclose Despite their Preferences

Compulsorily symmetrically reciprocal information sharing can be coercive. Mutually sharing details about ourselves is how we build relationships and intimacy with other people; however, this sharing should be done freely without coercion in order to actually achieve positive outcomes of closeness. Reciprocal sharing that leads to closeness does not need to be perfectly symmetrical in content or timing. Each user has a different background, life circumstance, and personal characteristics, which can influence what certain data actually reveals about them. For example, location data for someone who frequently visits specialized doctors or therapists could leak their health conditions, which they may prefer not to share. On the other hand, sharing location data with close friends and family while travelling could foster closeness as a means of sharing details about the trip and, notably, *without* leaking sensitive health data. The location sharing services I have used *do* enable this sort of asymmetrical sharing; however in both the context of online dating and OSIs, I found potentially coercive examples in which users could only see another user's freely disclosed information if they also shared their own (*e.g.,* questions on OKCupid where the answer can only be seen by other users who have answered the same question and OSI designs where turning of your OSIs also prevents you from seeing others'), and I additionally found that this *did* in some cases influence users to share information they would have preferred not to share. App designers should consider how technology can be used to help users organically navigate interpersonal relationships themselves rather than introducing barriers that create new types

of interpersonal tensions.

5.2 Extensions and Future Work

There is a great deal of additional research that could contribute to our understanding of U2U Privacy and the trade-offs that users face while engaging with technology. In Chapter 4, I have described planned continuation of the development of WYR, such as deploying it online and exploring its potential for use as an educational tool. Beyond this concrete planned future work, in this section I will describe more speculative, broad ideas for future work.

There is a huge variety of online dating apps, and these apps change significantly over relatively short periods of time. The understanding of online dating gained through my research was very broad. An analysis of the design space of online dating apps and how specific apps shape what users disclose and how they enable users to control their profile's audience (or not) would provide useful insight. One way to structure this analysis might first identify common user goals or tensions and then explore the ways in which popular online dating apps do or do not support these goals or ease these tensions. For example, tensions related to interacting with employers or colleagues emerged in the surveys and interviews discussed in Chapter 2 and in the online dating focused deployment of WYR (Chapter 4). A pertinent research question might ask: "How and to what extent do various online dating apps allow users to avoid their coworkers?" Only one app that I am aware of, "The League," explicitly addresses this by allowing users to import their LinkedIn connections. In my study, I found that participants described strategies they used in other apps, such as proactively finding and blocking their colleagues or avoiding using location-based apps while near work, but my work did not seek to systematically understand how specific apps address this tension beyond what participants spontaneously brought up.

There are many social features besides OSIs that could be studied across a variety of apps and app genres in order to understand whether the implementation of similar features in different apps is consistent, and how differences in design can impact disclosure. For example, typing indicators and read receipts are similar to OSIs in that they passively disclose

information when a user takes certain actions in an app (read receipts have been addressed from the standpoint of their impact on users [67]). Like OSIs, there is evidence that there are difficult-to-notice differences in how these features are implemented across apps [4] and what, if any, settings apps provide to enable users to control these features. Other social features or questions related to social features that I have identified, building on the types of nuanced differences that exist in the implementation of OSIs include: what happens when you send a friend request in different apps — can the sender's profile be seen before the request is accepted? Can the request be rescinded? Similarly, when users set up an account via Facebook, what actually happens if the app syncs friends — does it keep the friend list consistent, removing them in this app if you unfriend them on Facebook and/or adding them as you add new friends on Facebook? What happens to app and phone notifications if someone 'likes' and then 'unlikes' someone else's social media content (*e.g.,* a common fear is accidentally "liking" someone's very old content, which would reveal that you were "Facebook stalking" them) — does the notification persist? If so, does it specify who "liked" what?

My technical analysis of OSIs, descriptions of online dating apps, and the previously proposed analysis of a variety of social features all address only how these features were implemented at a single point in time. However, many apps add social features or change their implementation over time. In many cases, it may be difficult or impossible to know whether someone's incorrect understanding of how these features work(ed) represented a previous version of the app or a misunderstanding. That is, there is not currently a way to track the evolution of some of social features, particularly these specific low-level implementation details of social features, which I have shown can impact disclosure. A longitudinal study or the development of a tool or platform to track these changes would be an useful future contribution. Understanding and tracking the evolution of social features might be especially relevant in online dating apps, because many people use them intermittently (*e.g.,* stop using them while they are in a relationship and then resume use if the relationship ends). Thus, online dating users may feel they are repeatedly exposed to unfamiliar re-workings of

apps — and specifically apps where they already have an incentive to share sensitive information with broad audiences. Follow-on research questions might ask whether the evolution of these social features is occurring in reaction to user preferences or as a calculated, slow erosion of users' ability to maintain their own privacy.

In both my studies of online dating and OSIs, I considered only relationships between users who have approximately symmetrical access to app features. That is, the users were not specially priviledged or segregated from each other by any particular "role" in the app. However, there are many more categories and genres of apps with social features where this is not the case. Future work could explore what social features exist in dog walking apps such as Rover, babysitting or care apps such as Care.com, car-share apps like Uber and Lyft, and apps used in educational contexts such as UW's Canvas app. In these apps, usres are categorized as dog/baby sitters and clients, drivers and riders, or teachers and students, and the app itself may not allow one group of users to know what information they are broadcasting to the other group of users. For example, many of these apps allow users to rate or review others, and this rating or review may be invisible to the person it concerns. For example, babysitters may rate or discuss whether a client's children were well-behaved without the parent's awareness. Teachers in Canvas can see if and for how long individual students looked at certain course resources, but this would likely surprise the students. In these apps with hierarchies or categories of users, this kind of asymmetry in disclosure likely leads to broken privacy expectations in ways that are even more surprising and less controllable than the apps I have studied.

Finally, while my work has proposed some design recommendations, I have not implemented or tested any of these ideas in terms of how users would react to them. Also, while the design suggestions I have made were informed by a human-centered approach, co-design or participatory design with users could lead to more diverse and novel ideas for creating or changing apps to better balance users' desire to form connections with others by choosing to share information with their needs and preferences for also protecting certain information they want to keep private.

5.3 Final Words

In this dissertation, I have taken a human-centered approach to understanding how users control or attempt to control their privacy in social and communications applications. I began in Chapter 1 with two overarching research questions. In Section 1.3, I described how some previous work has addressed certain aspects of these questions. Then, in subsequent chapters, I describe the work that I have done as part of this dissertation. In Chapter 2, I studied users' privacy concerns in the specific context of online dating. U2U Privacy emerged organically as a key theme in participants' experiences in this context. That is, the most salient privacy goals that participants described involved how other users of online dating services might interpret or handle potentially sensitive information that they shared. In Chapter 3, I consider OSIs, which exist as a feature in many popular apps; while participants were familiar with these indicators, I found that current implementations of OSIs leave users app-dependent rather than app-enabled in terms of their ability to control how OSIs reflect on their self-presentation. In both of these contexts, I found that users face nuanced trade-offs whereby they have to choose between privacy and other goals for using these apps, services, or features. I also identified nuances in terms of how different groups of users are differently affected by technology designers' privacy choices. The projects described in these two chapters utilize traditional methodologies of surveys and interviews. Chapter 4 introduces Would You Rather, a novel methodology that I developed as part of my dissertation that directly addresses the trade-offs that users may encounter in their use of technology. My dissertation contributes concrete findings related to the application domain of online dating and the specific feature of OSIs, describes a design methodology for surfacing and understanding trade-offs related to U2U Privacy, and coalesces key U2U Privacy themes and best practices for design that are likely applicable beyond the specific contexts I have studied.

BIBLIOGRAPHY

[1] 15% of American adults have used online dating sites or mobile dating apps. pewrsr.ch/1SgNCZl. Accessed: 2016-10-22.

[2] The case for an older woman. blog.okcupid.com/index.php/the-case-for-an-older-woman. Accessed: 2016-10-22.

[3] Dark Patterns: inside the interfaces designed to trick you. www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you. Accessed: 2018-02-18.

[4] The iMessage dots explained - business insider. www.businessinsider.com/the-imessage-dots-explained-2016-1. Accessed: 2019-06-08.

[5] Ipsative — Wikipedia. en.wikipedia.org/wiki/Ipsative. Accessed: 2019-06-08.

[6] Is it ok to have read receipts on? www.buzzfeed.com/laraparker/spoiler-alert-its-not. Accessed: 2017-11-27.

[7] OKCupid about. www.okcupid.com/about. Accessed: 2016-10-22.

[8] Online dating survey instrument. homes.cs.washington.edu/ cobbc12/publications/ HowPublicIsMyPrivateLife_SurveyInstrument.pdf . Accessed: 2018-02-18.

[9] Researchers caused an uproar by publishing data from 70,000 OKCupid users. fortune.com/2016/05/18/okcupid-data-research. Accessed: 2016-15-09.

[10] Tinder. www.gotinder.com/press. Accessed: 2016-10-22.

[11] Two-alternative forced choice — Wikipedia. en.wikipedia.org/wiki/Two-alternative_forced_choice. Accessed: 2019-06-08.

[12] Why'd you push that button? www.theverge.com/whyd-you-push-that-button. Accessed: 2018-02-18.

[13] Would you rather — Wikipedia. en.wikipedia.org/wiki/Would_you_rather. Accessed: 2019-06-08.

[14] xkcd: Typing notifications. xkcd.com/1886. Accessed: 2017-11-27.

[15] Young job-seekers hiding their Facebook pages. www.cnn.com/2010/TECH/03/29/facebook.job-seekers . Accessed: 2016-10-22.

[16] Bumble — bumble photo verification — kiss catfish goodbye, 2014. Accessed: 2019-06-13.

[17] PositiveSingles STD dating site faces $16.5m penalty. web.archive.org/web/20141111143653/http://www.bbc.com/news/technology-29912279, 2014.

[18] Tourist sexually assaulted in Sydney by several men after meeting on Tinder. web.archive.org/web/20141010194852/http://www.news.com.au/national/tourist-sexually-assaulted-in-sydney-by-several-men-after-meeting-on-tinder/story-fncynjr2-1227083995690, 2014.

[19] Olympics and chill, 'A sexually charged time': Inside Rio Olympic's Tinder game where athletes are getting their swipe on. web.archive.org/web/20160815045954/https://www.thesun.co.uk/living/1588637/a-sexually-charged-time-inside-rio-olympics-tinder-game-where-athletes-are-getting-their-swipe-on/, 2016.

[20] What are digital traces? Me and my shadow, 2016. Accessed: 2016-15-9.

[21] People didn't know that their Instagram polls weren't anonymous and it's a total mess, 2017.

[22] App Annie about. www.appannie.com/en/about/, 2019. Accessed: 2019-05-13.

[23] Google Play Store. play.google.com/store?hl=en_US, 2019. Accessed: 2019-05-13.

[24] Alessandro Acquisti and Ralph Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *PETS*, 2006.

[25] Lalit Agarwal, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. Do not embarrass: Re-examining user concerns for online tracking and advertising. In *SOUPS*, 2013.

[26] Lujayn Alhddad. Read receipts feature in mobile platform: An investigation study based on social tie between the sender and receiver. 2015.

[27] Julio Angulo and Martin Ortlieb. WTH..!?! experiences, reactions, and expectations related to online privacy panic situations. In *SOUPS*, 2015.

[28] Daniel Avrahami and Scott E. Hudson. Communication characteristics of instant messaging: Effects and predictions of interpersonal relationships. In *CSCW*, 2006.

[29] Daniel Avrahami and Scott E. Hudson. Responsiveness in instant messaging: Predictive models supporting inter-personal communication. In *CHI*, 2006.

[30] Jared S. Bauer and Julie A. Kientz. Designlibs: A scenario-based design method for ideation. In *CHI*, 2013.

[31] James "Bo" Begole, John C. Tang, Randall B. Smith, and Nicole Yankelovich. Work rhythms: Analyzing visualizations of awareness histories of distributed groups. In *CSCW*, 2002.

[32] Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Comput.*, 2011.

[33] Igor Bilogrevic, Kévin Huguenin, Berker Agir, Murtuza Jadliwala, and Jean-Pierre Hubaux. Adaptive information-sharing for privacy-aware mobile social networks. In *UbiComp*, 2013.

[34] Courtney Blackwell, Jeremy Birnholtz, and Charles Abbott. Seeing and being seen: Co-situation and impression formation using Grindr, a location-aware gay dating app. *New Media & Society*, 2014.

[35] Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger, and Gernot Bauer. Falling asleep with Angry Birds, Facebook and Kindle: A large scale study on mobile application usage. In *MobileHCI*, 2011.

[36] Jed R Brubaker, Mike Ananny, and Kate Crawford. Departing glances: A sociotechnical account of 'leaving' Grindr. *New Media & Society*, 2014.

[37] Andreas Buchenscheit, Bastian Könings, Andreas Neubert, Florian Schaub, Matthias Schneider, and Frank Kargl. Privacy implications of presence sharing in mobile messaging applications. In *MUM*, 2014.

[38] Monica Caraway, Daniel A. Epstein, and Sean A. Munson. Friends don't need receipts: The curious case of social awareness streams in the mobile payment app Venmo. *CSCW*, 2017.

[39] John Carroll. Five reasons for scenario-based design. volume 13, page 11 pp., 02 1999.

[40] Shruthi Sai Chivukula, Jason Brier, and Colin M. Gray. Dark intentions or persuasion?: UX designers' activation of stakeholder and user values. In *DIS*, 2018.

[41] Camille Cobb and Tadayoshi Kohno. How public is my private life?: Privacy in online dating. In *WWW*, 2017.

[42] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *CHI*, 2005.

[43] Elena Francesca Corriero and Stephanie Tom Tong. Managing uncertainty in mobile dating applications: Goals, concerns of use, and information seeking in Grindr. *New Media & Society*, 2016.

[44] Lorrie Faith Cranor and Lawrence Lessig. *Web Privacy with P3P*. O'Reilly & Associates, Inc., 2002.

[45] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. The role of social influence in security feature adoption. In *CSCW*, 2015.

[46] Munmun De Choudhury, Scott Counts, and Eric Horvitz. Social media as a measurement tool of depression in populations. In *Websci*, 2013.

[47] Edward S. De Guzman, Margaret Yau, Anthony Gagliano, Austin Park, and Anind K. Dey. Exploring the design and use of peripheral displays of awareness information. In *CHI EA*, 2004.

[48] Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 2009.

[49] Sebastian Deterding, Andrés Lucero, Jussi Holopainen, Chulhong Min, Adrian Cheok, Annika Waern, and Steffen Walz. Embarrassing interactions. In *CHI EA*, 2015.

[50] Ravi Dhar and Itamar Simonson. The effect of forced choice on choice. *Journal of Marketing Research*, 2003.

[51] Christian Dindler and Ole Sejer Iversen. Fictional inquiry—design collaboration in a shared narrative space. *CoDesign*, 3(4):213–234, 2007.

[52] Trinh Minh Tri Do, Jan Blom, and Daniel Gatica-Perez. Smartphone usage in the wild: A large-scale analysis of applications and context. In *ICMI*, 2011.

[53] Madison Fansher, Shruthi Sai Chivukula, and Colin M. Gray. #Darkpatterns: UX practitioner conversations about ethical design. In *CHI EA*, 2018.

[54] Jody Farnden, Ben Martini, and Kim-Kwang Raymond Choo. Privacy risks in mobile dating apps. *CoRR*, 2015.

[55] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving SSL warnings: Comprehension and adherence. In *Proceedings of the Conference on Human Factors and Computing Systems*, 2015.

[56] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "a stalker's paradise": How intimate partner abusers exploit technology. In *CHI*, 2018.

[57] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *CSCW*, 2017.

[58] Anna-Katharina Frison, Philipp Wintersberger, and Andreas Riener. First person trolley problem: Evaluation of drivers' ethical decisions in a driving simulator. In *AutomotiveUI Adjunct*, 2016.

[59] Howard Gardner and Katie Davis. *The app generation: How today's youth navigate identity, intimacy, and imagination in a digital world*. Yale University Press, 2013.

[60] Jennifer L Gibbs, Nicole B Ellison, and Chih-Hui Lai. First comes love, then comes Google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, 2010.

[61] Erving Goffman. The presentation of self in everyday life. *American Journal of Sociology*, 1949.

[62] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile?: Technology, risk and privacy among undocumented immigrants. In *CHI*, 2018.

[63] David Gudelunas. There's an app for that: The uses and gratifications of online social networks for gay men. *Sexuality & Culture*, 2012.

[64] Jeff Hancock, Jeremy Birnholtz, Natalya Bazarova, Jamie Guillory, Josh Perlin, and Barrett Amos. Butler lies: Awareness, deception and design. In *CHI*, 2009.

[65] Jeffrey T. Hancock, Catalina Toma, and Nicole Ellison. The truth about lying in online dating profiles. In *CHI*, 2007.

[66] Pamela J. Hobart. New app the league helps you avoid coworkers while dating online, 2014. Accessed: 2019-06-13.

[67] Roberto Hoyle, Srijita Das, Apu Kapadia, Adam J. Lee, and Kami Vaniea. Was my message read?: Privacy and signaling on facebook messenger. In *CHI*, 2017.

[68] Jeremy Hsu. The strava heat map and the end of secrets. /www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/, 2018.

[69] Leslie K John, Alessandro Acquisti, and George Loewenstein. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, 2011.

[70] Maritza Johnson, Serge Egelman, and Steven M. Bellovin. Facebook and privacy: It's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, 2012.

[71] Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 2017.

[72] Amy Kraft. Tinder's new feature lets you play matchmaker. www.cbsnews.com/news/tinders-dating-app-feature-lets-you-play-matchmaker, 2016. Accessed: 2019-06-13.

[73] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. Who wants to know what when? Privacy preference determinants in ubiquitous computing. In *CHI EA*, 2003.

[74] Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. Analyzing facebook privacy settings: User expectations vs. reality. In *IMC*, 2011.

[75] Sonia Livingstone. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 2008.

[76] Kai Lukoff, Cissy Yu, Julie Kientz, and Alexis Hiniker. What makes smartphone use meaningful or meaningless? *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2018.

[77] Huina Mao, Xin Shuai, and Apu Kapadia. Loose tweets: An analysis of privacy leaks on Twitter. In *WPES*, 2011.

[78] Stevie Martin. How does Facebook suggested friends actually work. thedebrief.co.uk/news/real-life/facebook-suggested-friends-work/, 2017.

[79] Alice E. Marwick and danah boyd. I tweet honestly, i tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 2011.

[80] Alice E Marwick and danah boyd. Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 2014.

[81] Christopher M. Mascaro, Rachel M. Magee, and Sean P. Goggins. Not just a wink and smile: an analysis of user-defined success in online dating. In *iConference*, 2012.

[82] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *CHI*, 2017.

[83] Saul McLeod. What is conformity? www.simplypsychology.org/conformity.html, 2016. Accessed: 2019-05-31.

[84] Brittney McNamara. Olympics 2016: Closeted gay athletes outed by Daily Beast Grindr article. web.archive.org/web/20160921223540/http://www.teenvogue.com/story/straight-journalist-outed-closeted-gay-olympic-athletes-grindr, 2016.

[85] Brendan Meeder, Jennifer Tam, Patrick Gage Kelley, , and Lorrie Faith Cranor. RT @IWantPrivacy: Widespread violation of privacy settings in the Twitter social network. In *SNSP*, 2010.

[86] Z. Meng and M. Zuo. Why MSN lost to QQ in China market? different privacy protection design. In *ISA*, 2008.

[87] Alexander G. Mirnig and Alexander Meschtscherjakov. Trolled by the trolley problem: On what matters for ethical decision making in automated vehicles. In *CHI*, 2019.

[88] Neema Moraveji, Jason Li, Jiarong Ding, Patrick O'Kelley, and Suze Woolf. Comicboarding: Using comics as proxies for participatory design with children. In *CHI*, 2007.

[89] Bonnie A Nardi, Steve Whittaker, and Erin Bradner. Interaction and outeraction: instant messaging in action. In *CSCW*, 2000.

[90] Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 2007.

[91] Deirdre O'Brien and Ann M. Torres. Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, 2012.

[92] Remee Patel. This "would you rather" test will reveal if you're addicted to your phone. www.buzzfeed.com/remeepatel/this-game-of-would-you-rather-will-reveal-if-youre-addicted, 2017.

[93] Sameer Patil, Xinru Page, and Alfred Kobsa. With a little help from my friends: Can social navigation inform interpersonal privacy preferences? In *CSCW*, 2011.

[94] Iasonas Polakis, George Argyros, Theofilos Petsios, Suphannee Sivakorn, and Angelos D. Keromytis. Where's Wally?: Precise user discovery attacks in location proximity services. In *CCS*, 2015.

[95] Andrew G Reece and Christopher M Danforth. Instagram photos reveal predictive markers of depression. *EPJ Data Science*, 2017.

[96] Andrew G. Reece, Andrew J. Reagan, Katharina L. M. Lix, Peter Sheridan Dodds, Christopher M. Danforth, and Ellen J. Langer. Forecasting the onset and course of mental illness with Twitter data. In *Physics and Society*, 2016.

[97] Franziska Roesner, Brian T. Gill, and Tadayoshi Kohno. Sex, lies, or kittens? Investigating the use of Snapchat's self-destructing messages. In *Financial Crypto*, 2014.

[98] Tracii Ryan, Andrea Chester, John Reece, and Sophia Xenos. The uses and abuses of Facebook: A review of Facebook addiction. *Journal of Behavioral Addictions*, 2014.

[99] Douglas Schuler and Aki Namioka. *Participatory design: Principles and practices*. CRC Press, 1993.

[100] Saqib Shah. Hzone HIV dating app suffers massive data breach exposing 5,000 user accounts. web.archive.org/web/20151223153132/http://www.digitaltrends.com/social-media/hiv-dating-app-data-breach/, 2015.

[101] Jessica Staddon, David Huffaker, Larkin Brown, and Aaron Sedley. Are privacy concerns a turn-off?: Engagement and privacy in social networks. In *SOUPS*, 2012.

[102] Cali Stenson, Ana Balcells, and Megan Chen. Burning up privacy on Tinder. In *SOUPS (Posters)*, 2015.

[103] Eran Toch and Inbal Levi. Locality and privacy in people-nearby applications. In *Ubicomp*, 2013.

[104] Catalina L. Toma, Jeffrey T. Hancock, and Nicole B. Ellison. Separating fact from fiction: An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin*, 2008.

[105] Hui-Jie Tone, Hao-Rui Zhao, and Wan-Seng Yan. The attraction of online games: An important factor for internet addiction. *Computers in Human Behavior*, 2014.

[106] Chad Van De Wiele and Stephanie Tom Tong. Breaking boundaries: The uses & gratifications of Grindr. In *Ubicomp*, 2014.

[107] Daniel Victor. The Ashley Madison data dump, explained. web.archive.org/web/20150824053600/http://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html, 2015.

[108] Jessica Vitak, Cliff Lampe, Rebecca Gray, and Nicole B. Ellison. "Why won't you be my facebook friend?": Strategies for managing context collapse in the workplace. In *iConference*, 2012.

[109] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *SYM*, 1999.

[110] Jusik Woo. The right not to be identified: privacy and anonymity in the interactive media environment. *New Media & Society*, 2006.

[111] Peng Xia, Bruno F. Ribeiro, Cindy X. Chen, Benyuan Liu, and Donald F. Towsley. A study of user behavior on an online dating site. In *ASONAM*, 2013.

[112] Christopher C. Yang, Haodong Yang, Ling Jiang, and Mi Zhang. Social media mining for drug safety signal detection. In *SHB*, 2012.

[113] Douglas Zytko, Sukeshini A. Grandhi, and Quentin Jones. Impression management struggles in online dating. In *GROUP*, 2014.