Camille Cobb*, Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker

A Privacy-Focused Systematic Analysis of Online Status Indicators

Abstract: Online status indicators (or OSIs, *i.e.*, interface elements that communicate whether a user is online) can leak potentially sensitive information about users. In this work, we analyze 184 mobile applications to systematically characterize the existing design space of OSIs. We identified 40 apps with OSIs across a variety of genres and conducted a design review of the OSIs in each, examining both Android and iOS versions of these apps. We found that OSI design decisions clustered into four major categories, namely: appearance, audience, settings, and fidelity to actual user behavior. Less than half of these apps allow users change the default settings for OSIs. Informed by our findings, we discuss: 1) how these design choices support adversarial behavior, 2) design guidelines for creating consistent, privacy-conscious OSIs, and 3) a set of novel design concepts for building future tools to augment users' ability to control and understand the presence information they broadcast. By connecting the common design patterns we document to prior work on privacy in social technologies, we contribute an empirical understanding of the systematic ways in which OSIs can make users more or less vulnerable to unwanted information disclosure.

Keywords: Online Status Indicators, Usability, Mobile Ecosystem, Design, Information Leakage, Privacy

DOI 10.2478/popets-2020-0057
Received 2019-11-30; revised 2020-03-15; accepted 2020-03-16.

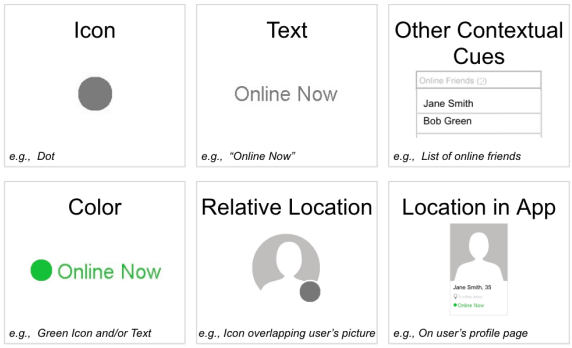

Fig. 1. OSIs can contain one or more abstract components: an icon, text, and other contextual cues. Each component can assume a specific color, relative location, and/or location within the app.

1 Introduction

Online Status Indicators (OSIs) are user interface (UI) elements that automatically broadcast information about when a user comes online or goes offline. When an OSI shows that a user is actively engaging with an app, it signals to others that the user is potentially available for conversation, multi-player gaming, and other social interactions. When an OSI shows that a user is offline, it indicates that the user may be unlikely to respond quickly or unavailable to connect. Although these uses of OSIs can improve a user's experience, prior work has found that OSIs can leak sensitive information [10] such as sleep-wake routines, workplace distraction, conversational partners, and deviations from daily schedules. These privacy concerns may be especially pronounced for people in vulnerable circumstances, such as those experiencing intimate partner violence, a devastating and widespread problem [29].

Despite the fact that OSIs are known to have problematic consequences for users, we currently lack a robust understanding of how and when OSIs project sensitive information. To what extent are OSIs present in popular apps and across app genres? How might their design and implementation affect the inferences that an observer can draw about a user's activities? In what ways and to what extent can users anticipate and control the information their OSIs broadcast?

***Corresponding Author: Camille Cobb:** Carnegie Mellon University, E-mail: ccobb@andrew.cmu.edu. Part of this work was done while the author was at the University of Washington.
Lucy Simko: University of Washington, E-mail: simkol@cs.uw.edu
Tadayoshi Kohno: University of Washington, E-mail: yoshi@cs.uw.edu
Alexis Hiniker: University of Washington, E-mail: alexisr@uw.edu

Scoped investigations of specific OSIs hint that the answers to these questions, in certain contexts, may be quite troubling in terms of under-explored risks to users. OSIs in WhatsApp can reveal how late a person stays at a party or who is talking to whom [10], and perpetrators of intimate partner violence have used OSIs to track their victims [19]. To date, prior work has investigated these questions in one-off contexts but has not documented the extent to which these trends are pervasive.

To understand how these risks manifest systematically and at scale, we examine OSIs across the mobile app ecosystem. Building on prior work that surfaces problems of broad social significance by holistically analyzing the mobile app marketplace [11, 27, 31], we seek to: 1) characterize the common ways in which OSIs are designed, and 2) draw on these design themes to assess the common privacy risks that OSIs pose to users. To these ends, we conducted a systematic analysis of 184 mobile apps, chosen to include popular apps from a varied genres, and a structured design review of a subset of 40 apps that use OSIs. We found that OSI design decisions clustered into subcategories within each of four different dimensions: appearance, audience, settings, and connection to ground-truth user behaviors. We evaluated the OSIs of all 40 apps against this taxonomy and differentiated these common design decisions according to their likelihood of affecting users' privacy.

OSIs are pervasive and valuable components of mobile apps, and quick-glance awareness of others' online status has become a standard feature that users have come to expect and rely on. Thus, discarding or avoiding OSIs due to potential privacy risks is not only impractical but at odds with the known value these features offer to users [28]. Instead, we seek to define with precision the risks that OSIs pose and identify the design mechanisms that act as vehicles for these risks. In doing so, we characterize the landscape of current OSI design, and we contribute design guidance for evolving OSIs to optimize for both protecting users' privacy and simultaneously preserving the value that users reap from sharing presence information with others.

2 Related Work

2.1 Understanding OSIs

A substantial amount of research, going back many years, has explored features that we would refer to as OSIs. In 2000, Nardi et al. studied 20 people's use of Instant Messenger (IM) at work [28]. They 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)). In their investigation of the benefits that IM can provide in the workplace, the authors 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 and also allowed the recipients to choose a good time to respond. The authors recommended that presence indicators provide *less* "awareness information" to give message recipients 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 of using "awareness" to improve online conversation and collaboration. For example, by making availability information and new messages only peripherally noticeable, IM conversations may become less distracting when users are busy [3, 12]. Other work proposed to help users navigate online conversations by incorporating data sources such as their online calendar and physical sensors to show and/or predict *availability* (or lack thereof) rather than mere presence [5, 21, 22]. Protocols such as XMPP [34] were developed to create a unified instant messaging experience (including OSIs) across multiple services. Although such protocols may be utilized for server-side implementation of OSIs, our work presents a client-side understanding.

We use this prior work to inform our understanding of the aspects that OSI designers and researchers have previously emphasized based on enhancing the potentially beneficial uses of OSIs. This allows us to take a more nuanced view of OSIs in order to draw attention to the tradeoffs between privacy and these other benefits rather than only identifying how OSIs could compromise privacy.

2.2 Privacy Risks of OSIs

Many studies have found that tracking OSI information (e.g., collecting data about what apps someone uses, for how long, and patterns of usage) can be used to infer substantially more about a user's real-world and online activity [6, 8, 10, 13]. For example, Buchenscheit et al. collected online status information for groups

of friends using WhatsApp. They found that online status can reveal the time people awaken or go to bed, their typical schedules, whether they deviate from those schedules, if they are using apps while at work, and, in some cases, which people within a group are conversing privately [10]. The authors report that participants discussed using OSIs to actively monitor or make inferences about their friends' behaviors, e.g. registering surprise about how late a friend stayed at a party. Further, 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 [13], indicating that the presence information conveyed by an OSI has the potential to reveal other sensitive details about an individual. Böhmer and colleagues, among others, further studied these and other patterns of app use and proposed leveraging them to create tools that offer just-in-time app suggestions to users [8]. Wide-scale deployment of such tools in conjunction with existing OSIs could exacerbate a hypothetical adversary's ability to infer where someone is located based on the app they are using.

Additional relevant concerns have also emerged in work whose *focus* was on topics or contexts besides online status. For example, Hancock et al. studied lies people tell online, in particular, "butler lies," which are frequently used to gracefully exit a conversation (*e.g.*, "Sorry, I've got to go to sleep now.") [20]. They hypothesized that since users typically tell butler lies to end a conversation, they might have preferred to avoid the conversation altogether; they recommend that apps let users determine whether *specific contacts* are able to see their online status. Several studies by Freed et al. found that easily accessible information on phones and in apps was leveraged by abusive partners [14, 15, 26]. Though they did not mention abuse of OSIs specifically, victims and survivors of domestic abuse might experience heightened privacy risks due to their partners' observations of their OSIs. In fact, one research study with a tangential focus *did* document an intimate partner violence survivor's concerns about OSIs [19]. In this work, we document the common themes in the design of current OSIs to provide an empirical base for evaluating the privacy risks apps create by adding this feature.

2.3 Systematic Analyses of Technical Design Spaces

In generating a taxonomy of OSI design implementations, we drew inspiration from previous Systematization of Knowledge papers, for example, those related to home IOT security, secure messaging tools, and proposed alternatives to passwords [1, 9, 33]. In these studies, the authors simplified a complex design space by identifying a small set of axes or categories along which a topic could be evaluated. For example, to evaluate password alternatives, Bonneau et al. identified 25 specific benefits that passwords offer, such as a negligible cost to users, and categorized them into usability, deployability, and security benefits [9]. These studies demonstrate how a systematized analysis can identify patterns, find gaps in literature or design exploration, and scaffold analysis of emerging ideas or implementations in their respective domains.

Other work has systematically reviewed mobile app ecosystems to better characterize the holistic state of these collective offerings. For example, Ross et al. evaluated the accessibility of mobile apps by conducting a review of 100 popular apps, finding that 100% had at least one of nine major accessibility flaws [31]. The authors framed this approach through an epidemiological lens, likening accessibility flaws to "diseases" and using their analysis to evaluate the overall "health" (with respect to accessibility) of the app marketplace.

Similarly, Callaghan and colleagues conducted a review of iOS and Android apps that claim to be educational for young children [11]. Despite the apps' marketing claims, the authors found that very few of the apps used evidence-based best practices that were conducive to learning, and most were unlikely to offer the educational benefits promised.

In other work, Meyer et al. reviewed 135 apps for children and report on a thematic analysis of the ways in which apps embed advertisements [27], such as commercialized characters, camouflaged game items, banner ads, and videos gating new game levels. In these and other investigations, researchers have broadly captured themes in the technical decisions and design choices that app developers are making across offerings. In doing so, they have distilled implications of broad social relevance, such as the accessibility of apps for disabled users, the educational value of mobile experiences, or the potential mechanisms by which children could be exploited by advertisements. Similarly, by holistically characterizing how mobile app developers currently con-

struct OSIs, we seek to illuminate thematic ways in which these interface elements might pose privacy risks.

3 Methodology

To create a taxonomy of OSIs, we first needed to identify a set of apps to evaluate. We identified 184 apps, 40 of which ended up having OSIs. Then, we applied an iterative analysis process to explore OSI design patterns in these 40 apps. This iterative process resulted in a rigorous set of analysis steps for each app, as shown in Figure 2 and described in Section 3.3. Primary analysis occurred between June 4 and September 14, 2018, and focused on Android apps. A secondary analysis, focused on iOS apps, occurred in November 2019. The scope of our observation 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 we observed in an app may not represent what all users would have seen during the study period.

While we considered automated analysis processes, such as analyzing the client-side app code, we quickly determined that critical aspects of OSIs can be observed only via real-time interactions between multiple user accounts. Such interactivity cannot be completely captured in client-side code. Additionally, automated analysis is well-suited for observing known patterns; however, our study goal was to identify previously unknown aspects of OSIs. Thus, we used a manual analysis process, which, although cumbersome, allowed us to incorporate several aspects of OSIs into our taxonomy that we would not have considered if we had been automating the app analysis process. Future work could automate observations of OSIs using the taxonomy we present, in order to observe a substantially larger set of apps or collect longitudinal data about changes to OSI designs, but these questions were beyond the scope of this work.

3.1 Identifying Apps for Analysis

Our goal was to comprehensively explore OSI design patterns for a set of apps representing a broad set of app genres and target users. However, the limitation of manual analysis required that we choose a manageable number of apps for analysis. Because we sought to generate a rich taxonomy of OSI designs across a *variety*

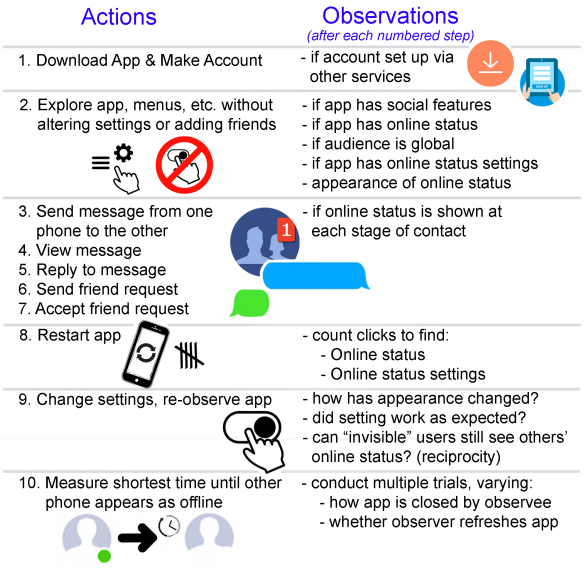

Fig. 2. Workflow for systematically analyzing OSI design patterns.

of popular apps, rather than to simply reach conclusions about OSIs in popular apps, we used the following diverse criteria to identify popular apps, with an intentional bias toward ones that we expected were likely to have OSIs:

- *Top-rated apps in general:* We included the top 50 free apps from the Google Play Store as of June 4, 2018, as archived on App Annie [2].
- *Top-rated apps by category:* We also included the 5 top-rated free apps in each of 13 categories and the top 10 free apps in the "social" category as of June 4, 2018, as archived on App Annie (for the Google Play Store [17]).
- *Novice users' app suggestions:* We 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 to have online status indicators" and 5 apps or services "that you think might have online status indicators." We included 40 apps suggested by these users that we could find in the Google Play Store.
- *App usage patterns:* We contacted the authors of a prior work [24], who shared data from 45 participants' phone usage behaviors, including which apps participants had used during a two-week period. We included the 48 apps used by at least 10% of participants.
- *Expert users' app suggestions:* Finally, we included 27 additional apps based on recommendations from expert users, including ourselves. For example, our expertise was informed by conversations with

teenagers at a university-sponsored CS outreach event separate from this study, who told us about the app Yubo.

In total, we identified 184 apps for analysis, listed in Appendix A.

3.2 Initial Analysis and Reliability Coding

Initial questions for first-round coding of all 184 apps, conducted by a single researcher, were: (*Q1*) Does this app have any social features? (*Q2*) Does this app have OSIs? (*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 required a paid account or special credentials to use. To explore OSIs despite this limitation, the researcher based this first round of 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 for analysis.

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. Researchers were in agreement about *Q2* except for one app, which only the primary coder identified as having OSIs. Excluding this app, coders found the same results regarding the ability to change app settings for OSIs (*Q3*). Coder agreement provided confidence that OSIs or OSI settings were not overlooked in any apps (i.e., no false negatives).

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 children's progress, but we 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 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 to be online/offline after opening/closing an app. A final round of analysis was performed on the 40 apps *with* OSI settings. Coders were unable to *directly* observe OSIs on Android in Steam and CoffeeMeetsBagel because doing so required paid accounts. The primary coder conducted a final round of analysis based on these themes using two factory-reset Android phones with new SIM cards and the following systematic analysis protocol:

1. Create Facebook accounts on both phones but do not connect them as friends. Some apps let users 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. Our OSI observations were made assuming that users *did* create accounts, and we did not classify the extent to which each app could be used without one.
2. Observe default settings for 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 shown in Figure 2, signing in through Facebook only when needed.
4. Finish app analysis for Facebook apps.
5. For some apps, we could not connect accounts without the accounts being Facebook friends. In this case, we 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, we 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 in to these apps 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 us carefully observe default app settings. 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 2), we measured timing information while phones were on the same wifi network, and we reported timing in coarse-grained buckets. There is substantial nuance in *how* we measured the time for users to appear as online or offline. Taking an adversarial mindset, we measured 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 2 denotes that if the adversary could *reliably* reduce the time it takes to see an updated OSI by repeatedly refreshing the page or closing and reopening the app, we *did* perform those actions. For most apps, we 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, we collected fewer and less precise measurements for apps with a time-to-offline that exceeded one hour. We did not collect timing measurements for apps where we 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.

Design Alignment between Android and iOS. To determine whether the characterizations we made were specific to the Android ecosystem or extended to other platforms, we analyzed the iOS version of the same 40 apps with OSIs. To conduct this comparative analysis, we:

1. Confirmed whether the original description of OSI appearance and scope matched the original analysis (the UI need not match in every way).
2. Confirmed whether the OSI of another user who was not yet a contact or connection could be seen.
3. Confirmed whether OSI settings functioned as in the original analysis.

As reported below, we encountered only minor differences in the design of OSIs on iOS versus Android. Thus, in our results we report on the original Android analysis, and we note differences between iOS and Android in Table 1 and 2 and Section 4.6.

4 Results

We now describe the design space of OSIs and the prevalence of common design patterns. Where applicable, screenshots were edited to replace identifying information from real users with generic profile photos and generic user information.

Of the 184 apps we analyzed, 116 had social features (defined in Section 3 and shown in black, red, or blue in the table in Appendix A). Of these 116, 40 had OSIs. Through our systematic technical review, we clustered the thematic features of these 40 apps (see Table 1). In this section, we describe these themes — including appearance, audience, settings, and connection to ground-truth behaviors. In Section 5, we return to these themes, considering them from a privacy threat-modelling perspective, but this section seeks only to describe the findings of our analysis.

4.1 Terminology

Prior work used a variety of terms—such as "online status," "active/activity status," "presence," "availability," or "last seen"—to describe what we refer to as an OSI; some apps did not explicitly name the feature at all. Here, we condense this breadth, and we define the term *Online Status Indicator (OSI)* to be 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, without deliberate action by the user, as they 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 we included these OSIs in our analysis.

For the remainder of this section, we refer to both *online status* and *online status indicators (OSIs)*. We 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 considerable amount of time for an app to reflect that someone has stopped using it, in which case the 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 referring to actual behavior, we use longer phrases, such as "whether the user is online" or "that the user is active."

In apps that include configurable settings for OSIs, we generally refer to the OSI as being "on" or "off" de-

	AUDIENCE			SETTINGS	APPEARANCE *Many apps show online status in more than one way. This table conveys only predominant presentations. Caveats are discussed inline or shown in other figures.*				TIMING	
	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 ***	ONLINE APPEARANCE	LAST ONLINE TIME	CLICKS TO SEE AN ONLINE STATUS	VISIBILITY OF SELF	TIME TO ONLINE *	TIME TO OFFLINE *
App *(App description)*	Typical, Sub-area, or Cross-app	● (Friends/connections), ○ (Global), or Other	Yes or No	Yes or No	● (Green dot), Text, or Other	Approximate or Exact	0 to 3 or Other	Yes or No	• (A few seconds), ● (A few minutes), -- (Not able to measure)	
Battle.net *(Gaming Chat)*	Cross-app (w/ Hearthstone)	●	Yes	Yes	●	Approximate	0	Yes	•	several hours
Canvas *(Education)*	Sub-area	Anyone w/ access to group chat (restricted)	No	No	●		3	Yes	•	•
Coffee Meets Bagel *(Dating)*	Typical	○	Yes	No	Clock icon and text **	Approximate	Must pay	No	--	--
Discord *(Gaming Chat)*	Typical	●	No	Yes	●		0	Yes	•	●
Facebook *(Social Media)*	Cross-app (FB Grouping)	●	No	Yes	●		0	No	•	●
Facebook Lite *(Social Media)*	Cross-app (FB Grouping)	●	No	Yes	●		0	No	•	10-60 minutes
Google Docs or Google Sheets *(Productivity)*	Sub-area	Anyone w/ access to doc or sheet	Yes	No	Cursor with username appears in doc; username in list of active users		1	No	•	•
(Google) Hangouts *(Chat)*	Typical	●	No	Yes	Text	Approximate	1	No	•	10-60 minutes
	Sub-area	Other person in conversation		No	Opaque thumbnail of profile picture, becomes transparent if not in sub-area		0 once in sub-area	No	•	•
Grindr *(Dating)*	Typical	○	No	No (Android); Yes, "new" for paid users (iOS)	●	Approximate	0	Yes	•	10-60 minutes
Happn *(Dating)*	Typical	○	Yes	No	Text	Approximate	1	No	--	--
Hearthstone *(Gaming)*	Cross-app (w/ Battle.net)	●	Yes	Yes (only via Battle.net app)	Text	Approximate	1	No	•	several hours
Hike *(Chat)*	Typical	●	No	Yes	Text	Exact	1	No	•	•
imo *(Chat)*	Typical	●	No	Yes (Android); "Last Seen" Settings (iOS)	Text	Exact	1	No	•	●
	Sub-area	Other person in conversation		No	Thumbnail of profile picture has teal border if online		0 once in sub-area	No	•	•
Instagram *(Social Media)*	Typical	●	Yes	Yes	●	Approximate	1	No	•	●
JOYRIDE *(Dating)*	Typical	○	Yes	No	●	Approximate	0	Yes	--	--
Jurassic World Alive *(Gaming)*	Typical	●	Yes	No	Orange dot for online, green dot for in-game		1 (Android); 2 (iOS)	No	•	●
LinkedIn *(Employment)*	Typical	No one, but app automatically changes to ● after some use *	Yes	Yes	●		2	Yes	•	●
Marco Polo Video Walkie Talkie *(Video Chat)*	Typical	○	No	No	Text	Approximate	2 (Android); 0 (iOS)	No	•	●
Match *(Dating)*	Typical	○	Yes	No	●	Approximate	0	No	--	--
(Facebook) Messenger *(Chat)*	Cross-app (FB Grouping)	●	Yes	Yes	●	Approximate	0	Yes	•	●
(Facebook) Messenger Kids *(Kids' Chat)*	Typical	●	Yes	No	●	No info (Android); Approximate (iOS)	0	No	●	●
(Facebook) Messenger Lite *(Chat)*	Cross-app (FB Grouping)	●	Yes	Yes	●	Approximate	0	Yes	•	●
MyFitnessPal *(Fitness)*	Typical	●	Yes	No	Text	Approximate	2	Yes	--	--
OfferUP *(Classifieds)*	Typical	○	Yes	No	Text	Approximate	2	No	--	--
OkCupid *(Dating)*	Typical	○	Yes	No	●		0	No	•	10-60 minutes
Plenty of Fish (POF) *(Dating)*	Typical	○	No	No	Text		1	No	--	--
PUBG MOBILE *(Gaming)* *	Typical	●	Yes	No	Text	Approximate	1	No	•	●
ROBLOX *(Gaming)*	Typical	○	No	No	Blue dot for online, green dot for in-game		2 (Android); 0 (iOS)	Yes	•	10-60 minutes
	Sub-area	Anyone w/ access to mini-game (most are public)		No	Presence in list of users in sub-area		1 once in sub-area	Yes	•	•
Skype *(Chat, Video Chat)*	Typical	●	Yes	Yes	●	Approximate	1 (Android); 0 (iOS)	Yes	•	•
Slack *(Chat, Work)*	Sub-area	Anyone w/ access to workspace (restricted)	Yes	Yes	● or other colors if different "theme" chosen; triangle for single-channel guests		1	Yes	•	•
Steam *(Gaming) Observed only on iOS*	Typical	●	No (& must sign up in browser)	Yes	Text	Approximate	0	No	•	•
Telegram *(Chat)*	Typical	● (Android); ○ (iOS)	No	Yes (but not functional on iOS)	Text	Exact (Android); Approximate (iOS)	0	Yes	•	•
Tumblr *(Social Media)*	Typical	○	No	Yes	●	Approximate	3 (Android); 1 (iOS)	No (Android); Yes (iOS)	●	10-60 minutes
Twitch *(Gaming, Chat, Livestreams)*	Typical	●	No	Yes	●	Text, grey dot	1 (Android); 2 (iOS)	No	•	10-60 minutes
Viber *(Chat)*	Typical	○	No	Yes	Text	Approximate	1	No	●	●
Waze *(Navigation)*	Typical	●	No	Yes	Text, green line	Approximate	3	No	●	●
WhatsApp *(Chat)*	Typical	○	No	"Last Seen" Settings	Text	Exact	2	No	•	•
Words with Friends (classic) *(Gaming)*	Typical	○	Yes	No	●	Approximate	0	No	●	10-60 minutes
Yubo *(Chat, Social Media)* *	Typical	●	No	No	●	Exact	1	No	•	•
Zoosk *(Dating)*	Typical	○	Yes	No	● with a thin white circle inside		0	No	--	--

* Observed only in original app analysis (Android OS, unless otherwise specified)

** Observed only via other sources (e.g., online image searches, app store screenshots)

*** See Table 2 for additional details about apps with OSI settings

Table 1. A simplified description of design patterns in 40 apps with OSIs.

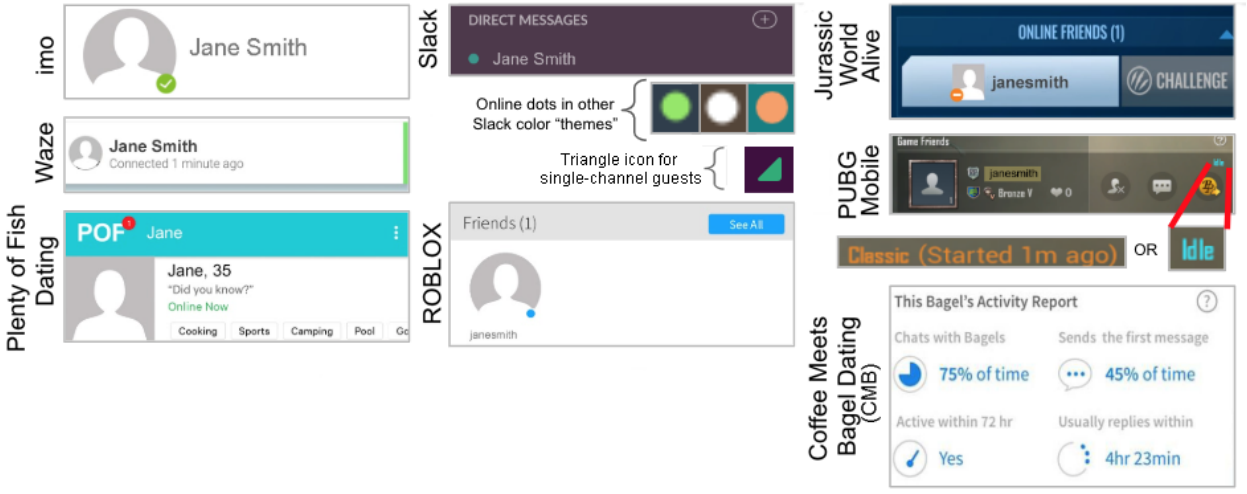

Fig. 3. Beyond simple green dots, apps used a wide variety of icons and text to show that a user was currently online.

pending on whether the app displays the icon and updates its appearance to reflect the user's online status. Where necessary, we 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 5.1, where we describe the apps for which an adversary could detect whether someone has turned off their OSI or is *actually* offline.

4.2 OSI Appearance

We found that the appearance of OSIs (for online *or* offline users) consisted of a subset of the abstract components shown in Figure 1. In this subsection, we describe the appearance of OSIs when users were online.

OSI Icons. We encountered a number of themes in the ways that apps indicated that a user was online. The most common (in 21 of 40 apps) was the use of a green dot. In many cases, the dot was placed close to a user's name or profile picture thumbnail (sometimes overlapping it) or elsewhere on a user's profile page. The appearance of the green dots varied across apps. For example, the "imo" app's green dot had a white check mark in it (Figure 3), and apps used various shades of green, even in apps made by the same company (for example, see Facebook and Messenger in Figure 4).

Although approximately half the apps signaled online status with a green dot, we also encountered a long tail of alternative representations (see Figure 3), including a diverse range of icon shapes and colors. For example, CMB used a clock-like icon (and text) to indicate whether the user had been online in the past 72 hours; Jurassic World Alive and ROBLOX used orange and

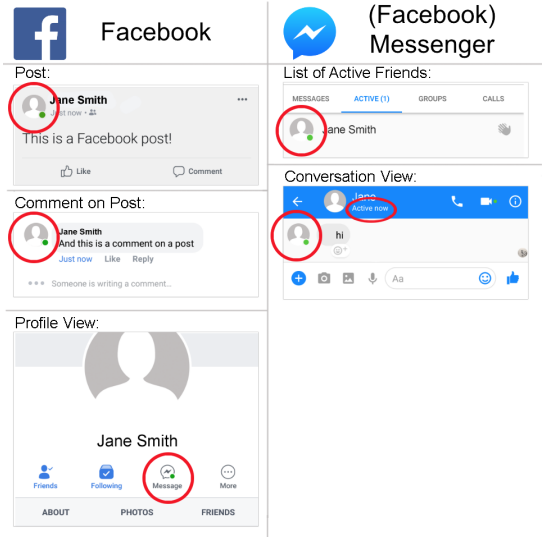

Fig. 4. In Facebook Apps (i.e., Facebook, Facebook Lite, Messenger, and Messenger Lite), OSIs appeared in several places in the app. Shown here are green dot OSIs in/on a post, comment, user's profile, list of online friends, and conversation view.

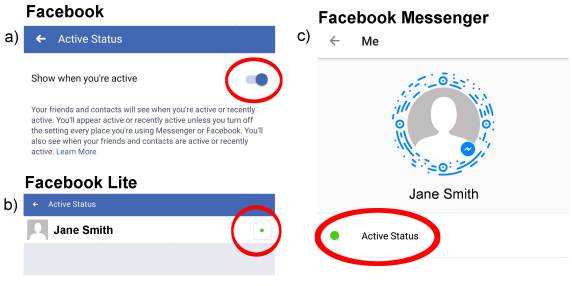

Fig. 5. Even though Facebook, Facebook Lite, and Facebook Messenger are made by the same company, their OSI settings did not share a consistent appearance.

blue dots to convey that the user had the app open. OSIs for users with limited permissions (referred to as "single-channel guests") in Slack workspaces used a triangle icon instead of a dot. Additionally, Slack allowed users to customize color schemes, which affected the color of OSIs (Figure 3). Thus, despite the common use of round green icons, nearly half of all apps used OSIs that deviated from this standard.

OSI Text. Several apps used text such as "Online Now" or "Active" in place of or in addition to an icon to represent online status. For example, POF Dating used a text-based OSI with no icon, but the text was colored green, reminiscent of the green icons in other apps (Figure 3). At times, this text was used to disambiguate the information conveyed by an OSI or convey more detailed information about what a user was doing. For example, Hearthstone, Battle.net, ROBLOX, and PUBG Mobile all used text to specify more about what users were doing in the app (e.g., which game they were playing), and Hangouts and Battle.net used text to convey whether a user was accessing the app via a mobile device. We discuss how these design choices contribute to an adversary's ability to make inferences about a target in Section 5.1.

Other Facets of OSI Appearance. Thirteen of 40 apps let users see their own OSIs. For example, the Facebook Messenger screenshot in Figure 5 (c) shows a green dot near the account owner's own name and profile picture. Further, we observed two apps that actively notified users when their friends came online. Facebook Messenger displayed a banner that said "[friend's name] is active now." Marco Polo Video Walkie Talkie had a similar feature and, although it did not have online status settings, it let users exclude themselves from these "activity updates."

OSI Appearance for Offline Users. When OSIs change to show that a user is offline, any text and/or icons may disappear or change in some way. Figure 6 shows examples of offline versus online users' OSIs. Because this transition manifests differently in different parts of the app, we did not systematically observe all possible offline OSIs in each app (e.g., offline users could appear differently in each of the Facebook and Messenger pages shown in Figure 4). When users were offline, 25 of 40 apps specified how long ago the user was online. Of those 25 apps, 5 revealed exactly what time the user was last online, and 16 gave an approximation, such as "last seen 4 hours ago." We return to these findings in Section 5.1 to explore how they affect whether a user could *covertly* turn off their OSI.

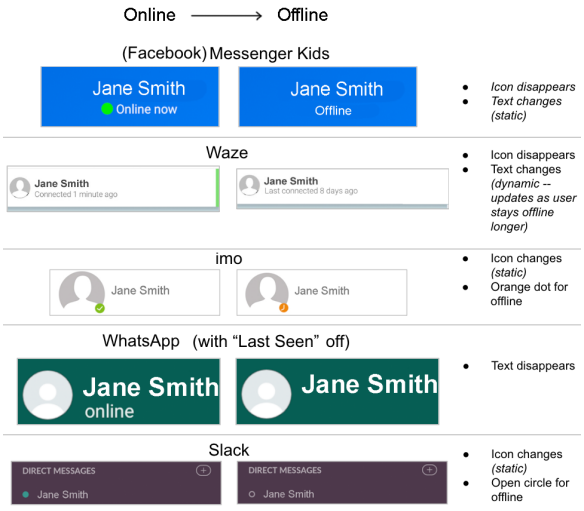

Fig. 6. Examples of online versus offline OSIs in several apps. Icons and/or text disappeared or changed when users went offline. If the icons or text changed, they did so either statically or dynamically. That is, in some cases, the text or icon continued to change as the user stayed offline, typically to indicate how long the user had been offline.

4.3 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 OSI audience. The right-middle and left-bottom images in Figure 7 illustrate typical OSIs visible only to connections versus to all other users, respectively.

Fifteen apps exposed OSIs to *all* other users of the app by default. Twenty-one apps had OSIs with default visibility only to connections. Of these, 8 let users sign in or sign up via another service, such as Facebook, typically syncing friends from Facebook to the new app. LinkedIn did not show online status to *anyone* initially; however, audience settings were automatically updated to make OSIs visible to connections. It was not obvious and beyond our research scope to understand what prompted this change.

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

and *Cross-App*, illustrated in the left-middle and right-bottom images in Figure 7, respectively. As discussed in Section 5, a narrower scope typically implies a smaller audience but might reveal more details about the user's behavior within an app.

Three apps had *only* Sub-Area OSIs: Slack within its workspaces, Canvas for its discussion boards, and Google Docs or Sheets for shared documents. Three apps had both *Typical* and *Sub-Area* OSIs: Hangouts and imo had conversation-level indicators that revealed when a chat partner was viewing the conversation, as shown in Figure 8; ROBLOX showed 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 Hangouts, only connections could see Typical OSIs; however, conversational Sub-Area OSIs revealed when someone was viewing a conversation that they had not initiated and had not yet replied to (replying caused the users to implicitly become contacts, after which the Typical OSI was visible as well). In all apps we analyzed, mutual presence in a sub-area was sufficient to describe the audience of a Sub-Area OSI, though some apps restricted sub-area access.

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 we studied had Cross-App OSIs: (1) Battle.net and Hearthstone, and (2) Facebook, Messenger, Facebook Lite, and Messenger Lite. We identified these sets of apps from personal use and knowledge of the apps rather than systematic analysis, so it is possible that other apps had Cross-App OSIs that we labelled Typical OSIs. In both of these groups of apps, the same account was used to access all apps. In terms of audience, this meant that "friends" or other connections were consistent across apps (i.e., Facebook friends match Messenger contacts). However, this behavior may still surprise users and, as related in Section 4.4, other aspects of Cross-App OSIs may place additional cognitive load on users.

4.4 Settings

All apps but LinkedIn had OSIs turned on by default. As shown in Table 2, 20 apps provided settings that let users turn off or hide their OSIs so that they no longer corresponded to their actual app/service use. This could mean that the OSI disappeared completely, changed to show that the user had turned it off, or that the user

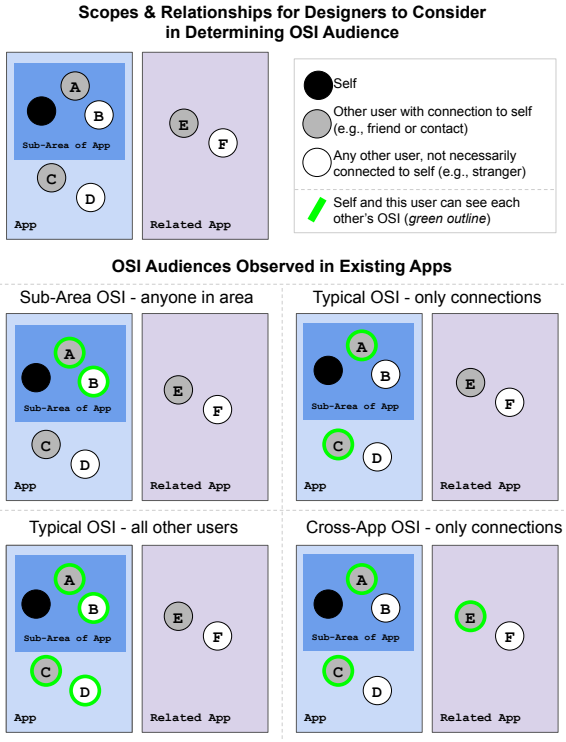

Fig. 7. OSI designers should consider which other users should be able to see someone's online status and under what conditions, in terms of: (1) *relationship* — whether users are connected as friends, contacts, etc., and (2) *scope* — "where" in the app the users are relative to each other. OSIs visible 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 at the bottom show default OSI audiences we observed in existing apps.

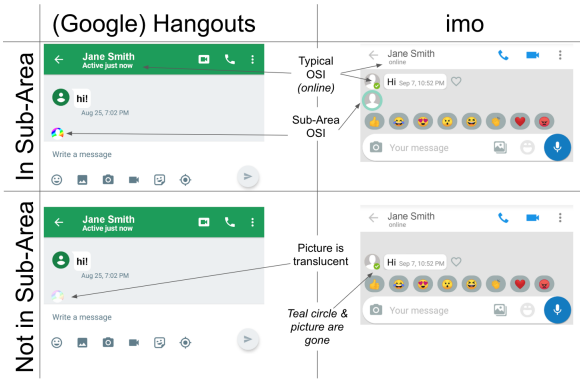

Fig. 8. Hangouts and imo had separate OSIs with Typical scope and Sub-Area scope showing other users' presence in a conversation.

APP	CLICKS TO TURN OFF ONLINE STATUS	SETTINGS PROPAGATION	RECIPROCITY	AUDIENCE OPTIONS	AVAILABILITY OPTIONS
Battle.net	3	Yes, to Hearthstone	No		Online, Away, Busy, Appear Offline
Discord	3	n/a	No		Online, Idle, Do not disturb, Invisible
Facebook	6	No	Yes		
Facebook Lite *No iOS version*	5	No	Yes		
(Google) Hangouts *Only applies to typical OSI for this app; sub-area OSI does not have settings*	5 (Android); 3 (iOS)	n/a	No		
Grindr *Settings added between Nov 2018 and Nov 2019 to both iOS and Android OS*	3	n/a	Not able to observe		
Hike	5	n/a	Yes	Everyone, Friends and Contacts, Friends, Specific People, Nobody	
imo *Only applies to typical OSI for this app; sub-area OSI does not have settings*	4 (Android); 5 (iOS)	n/a	No	Everyone, Contacts, Nobody	
Instagram	5 (Android); 6 (iOS)	n/a	Yes		
LinkedIn	5 (Android); 6 (iOS)	n/a	Yes	All LinkedIn Members, Connections Only, Nobody	
(Facebook) Messenger	4	No	Yes		
(Facebook) Messenger Lite *No iOS version*	5	No	Yes		
Skype	3	n/a	No		Active, Do not disturb, Invisible
Slack	3	No, not to other "workspaces"	No		
Steam *Observed only on iOS*	3	n/a	No		
Telegram *Changing settings did not have any effect in the Nov 2019 follow-up analysis*	5 (Android); 4 (iOS)	n/a	Yes	Everybody, Contacts, Specific People, Nobody	
Tumblr	5	n/a	No		
Twitch	4 (Android); 6 (iOS)	n/a	No		Online, Busy, Invisible
Viber	6 (Android); 4 (iOS)	n/a	Yes		
Waze	3	n/a	No		
WhatsApp Messenger *Online status cannot be turned off in WhatsApp; this row refers to the "Last Seen" setting in WhatsApp*	6 (Android); 5 (iOS)	n/a	Yes	Everyone, Contacts, Nobody	

Table 2. Properties of apps **with** OSI settings.

appeared offline indefinitely. Section 5.1 describes these differences in greater detail.

The design and implementation of OSI settings varied across apps, including similar apps made by the same company. For example, Figure 5 shows OSI settings in Facebook (a) and Facebook Lite (b), which were reached through similar but not identical settings menus; users reached the equivalent setting in Facebook Messenger (c) by clicking on the green dot in a non-menu interface. Figure 9 shows screenshots of settings menus for four additional apps. Waze (a) was the only app for which a toggle was turned *on* rather than *off* to prevent others from seeing online status updates. LinkedIn (b) was the only app that explicitly prompted users to notice OSIs and consider changing their settings; however, as previously noted, this cue was accompanied by an automatic change that made the OSI visible to connected users. WhatsApp (d) had a "Last Seen" option in its privacy settings, but this only determined whether the last online time was shown; it was not possible to prevent others from seeing whether you were *currently* online. This may be especially unexpected since four other apps (Hike (c), Hangouts, imo, and Telegram) also had a "Last Seen" setting that *did* turn off OSIs.

Locating OSI Settings. An imperfect measurement of how easily discoverable these controls were is the number of clicks it took upon opening the app to turn off OSIs. This number ranged from 3 to 6 clicks. Of the 18 apps that let users change their *Typical* OSI settings within an app, the settings for 9 apps were found in a "privacy" menu or list. In Twitch, users had to choose a menu option labelled "account" *instead* of "privacy" to find online status settings (Figure 10 b). Battle.net, on the other hand, let users change OSI settings directly from their profile via a small arrow next to the OSI icon rather than navigating through menus (Figure 10 a).

Controlling OSI Audience or "Availability." Four apps (Hike, imo, LinkedIn, and Telegram) let users specify the audience for their OSI in terms of relationship, specifically choosing from groups listed in Table 2. Hike and Telegram further enabled users to specify which *individuals* could or could not see their online status updates. The browser version of Facebook *did* let users control OSI visibility for specific subsets of friends, but this was not the case for Android or iPhone Facebook apps. Four other apps allowed a greater range of expression in terms of availability (e.g., "idle," "do not disturb," or "invisible" in Discord).

Do OSI Settings Propagate? For several apps, we were able to observe whether OSI settings propagated to other apps or sub-areas. Hearthstone's OSIs could not be turned off from within the Hearthstone app, but they *could* be turned off by turning off OSIs in the Battle.net app (thus, the settings propagated between apps). When users turned off Facebook app OSIs, an explicit policy informed them that settings were separate for each app and/or device. That is, settings *did not* propagate across apps or devices for Facebook. Online status in Slack did not propagate between workspaces. The study scope did not include non-mobile apps, but since we personally use Slack on multiple devices, we anecdotally observed that settings for a particular Slack workspace *did* propagate between devices.

Reciprocity. For 10 apps with OSI settings, users could still view others' OSIs even if they had turned off their own (i.e., the app did not provide *reciprocity*), as shown in Figure 11. Viber, which had reciprocity, let 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.

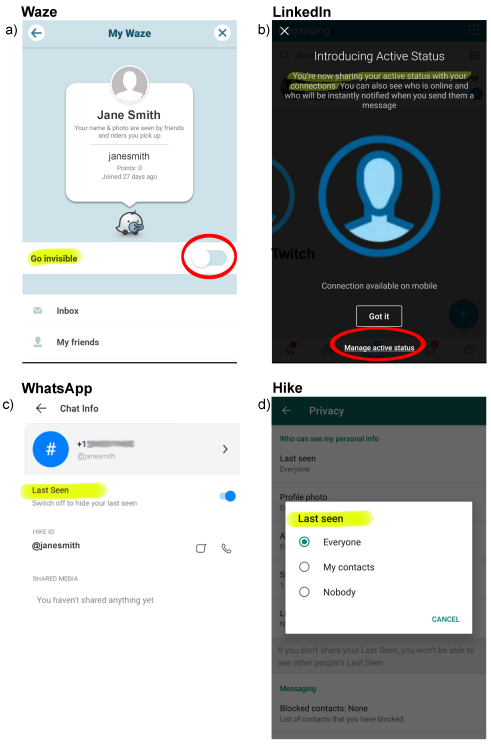

Fig. 9. Screenshots related to OSI settings in Waze, LinkedIn, WhatsApp, and Hike. Waze was the only app where users toggled a setting to "on" to avoid appearing as online. LinkedIn was the only app that prompted users about OSI settings. Although both WhatsApp and Hike had a "last seen" setting, the functionality of this setting was not the same.

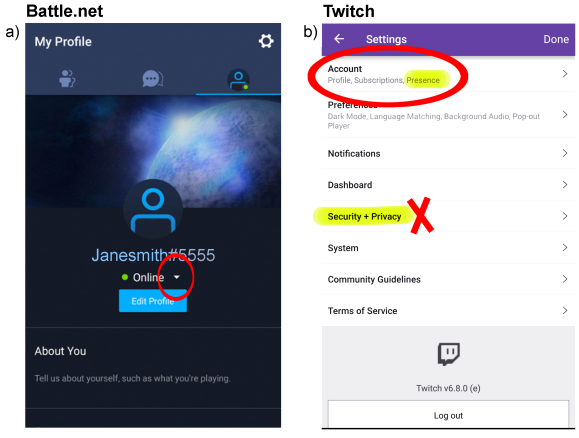

Fig. 10. Battle.net users could view their OSI and change their OSI settings directly from their profile page view. Twitch users may have found it unintuitive that OSI settings were *not* in the Security and Privacy menu.

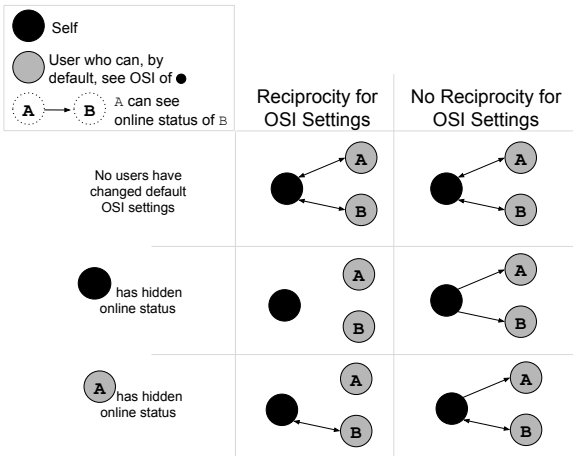

Fig. 11. Reciprocity of OSI settings means that a user cannot see others' OSIs if they choose to turn off their own.

4.5 Observed OSI Compared to Ground Truth User Behavior

OSIs do not always faithfully represent whether a user is *actually* online or offline. Disconnects between users' OSIs and their actual behavior may be caused by users setting their OSIs to offline or by latency in OSI updates as users come online or go offline.

We report the time to appear as online or offline in coarse-grained buckets in Table 1. For all apps, the OSI updated as fast or faster when users came online compared to when they went offline. In most apps and for all Sub-Area OSIs, the OSI reflected actual app use within just a few minutes. Some apps showed only whether a user had been online within the previous hour, day, or more (e.g., 72 hours in CMB). We discuss in Section 5.1 how this information, along with several other factors, affects privacy.

4.6 Comparing OSIs on iOS and Android

The majority of differences between OSIs on iOS and Android pertained only to the number of clicks required to see an OSI or find OSI settings. However, more substantial differences existed in Grindr, imo, Telegram, and FB Messenger Kids, as reported in Tables 1 and 2. For example, a Grindr feature let paid users appear "invisible," which the app UI specified was new. Whether the differences were due to design inconsistencies, actual differences between Android and iOS, or changes to both Android and iOS over time, this follow-up analysis demonstrated that OSIs in most apps were *relatively* consistent. More substantial differences may exist be-

tween desktop or browser and mobile versions of apps and should be explored in future work.

5 Discussion and Design Recommendations

We found great diversity in OSI appearance, default audience, settings, and connection to actual user behavior in existing apps. The variance of OSI design and implementations across apps leads to vast inconsistencies in how users' activity was represented and shared, which likely would make it difficult for users to anticipate and/or control how their online status will be reflected to others. In this section, we first discuss how OSI implementations could enable or hinder adversarial observations of another user's OSI. Building on this discussion and informed by prior work and prevalent OSI patterns we identified across apps, we present a set of suggestions to guide designers toward implementing more consistent and privacy-conscious OSIs. Finally, we consider how our findings lead to novel ideas for OSI implementations that go beyond existing designs.

5.1 Threat Modelling OSI Designs

We now consider how the OSI design decisions we document might affect the privacy of a user targeted by an adversary.

Adversarial Inferences about User Behavior. The inferences an adversary can make about a target depend upon the accuracy with which they can infer ground truth app use and other information that the OSI conveys about the target's behavior.

The granularity with which an adversary can monitor a target's app use is a function of how precisely an OSI reflects changes in a user's behavior, including both the *amount of time* it takes for users to appear online or offline *and* the *consistency* of this time span. Consider Hangouts as a concrete example of how an adversary might leverage timing and consistency information to track someone's app use. Users consistently appeared online almost immediately and appeared offline 15 minutes after they stopped using the app. An adversary would know that the target was *actually* online around the time they came online and *actually* quit the app approximately 15 minutes before their OSI changed to offline. If the target user appeared 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 could not know exactly how many times or when the target opened and closed the app. On the other hand, in apps like Slack and Google Docs, whose OSIs update almost immediately as users come and go from the app, an adversary could infer behavior with higher confidence and precision.

As noted in Section 4.2, some text-based OSIs convey more information than merely whether a user is online or offline, for example, whether the user is accessing the app via a mobile or desktop device (as in Hangouts) or what they are doing within the app (as in Battle.net). The scope of an OSI can also suggest what a target might be doing in the app. Sub-Area OSIs implicitly tell users that they are both accessing the same sub-area of an app. Cross-App OSIs do not necessarily reveal as much as Typical or Sub-Area OSIs about what the observed user is doing, although in practice we observed that the former sometimes revealed which app the observed user was accessing (e.g., Facebook showed users as "Active on Messenger" or "Active on Facebook").

Additionally, simply using certain apps might leak information. For example, coming online to a dating app for the first time in a while might lead an adversary to conclude that the observed user is newly single or considering cheating; seeing that a user has opened Waze on a weekday evening might suggest that they are leaving work. Thus, although OSIs in frequently used apps might provide more opportunities for adversaries to monitor use, this does not imply that OSIs in rarely used or less popular apps pose a smaller privacy risk.

Detecting Changes to OSI Settings. Further exploring OSI trustworthiness, an adversary may wish to know whether a target has turned off their OSI. If turning off an OSI changes its appearance such that it looks *different* than if they had their OSI on (but were offline), it would be obvious *that* the target has changed the OSI setting but potentially impossible to determine *whether* they are currently online. For example, it was clear in WhatsApp that a user had turned off the "last seen" setting because the area that normally showed the last online time was blank when the user was offline.

In apps where turning off an OSI causes the OSI to appear as though the target were offline, it would be harder but not impossible to detect *that* the target user had changed this setting. Taking the previous example of Hangouts, although users consistently appeared offline 15 minutes after they actually went offline, turning off the OSI caused a user to appear offline *immediately*. To ensure that others could not detect when they turn off OSIs, users would need to stay online for 15 minutes

before they actually changed the setting while refraining from observable app activity.

Adversarial Ease of Monitoring OSIs. Although we recognize that some users (e.g., people experiencing domestic abuse) may need to protect themselves against highly motivated adversaries, OSI designs that make it more difficult for an adversary to monitor OSIs may discourage malicious behavior. Likewise, certain OSI designs could enable even casual observers to draw conclusions about a user's behavior.

As discussed in Section 3, an adversary who wants to monitor someone's OSI with high precision and accuracy might need to take certain actions, like repeatedly refreshing or restarting 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 descriptive text, while always technically correct, was phrased so that a single OSI observation provided only vague insight into a user's actual behavior: if the user was online, multiple refreshes of their profile would display either "Active in the last hour" or "Active in the last 2 hours."

Apps that show precisely how long ago someone was online create 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.

Ability to Target Specific Users. Although 14 apps expose OSIs to all other users by default, it may have been nontrivial to target a specific person. For example, in dating apps like Grindr and Match, profiles (which include OSIs) were visible to nearby users, so an adversary would see *someone's* OSI, though it would be difficult to look up *specific* users. WhatsApp users could be looked up from their phone numbers. Depending on the adversary's relationship to the target user it may be easier or harder for them to see a specific target user's OSI in these apps.

Automated and/or Scaled Attacks. All of the data collection in this work was done manually, representing the capabilities of an adversary who may be committed but is not particularly technically savvy; however, the implications we draw also apply to an adversary who automatically programmatically collects online status information about a target user (e.g., by using underlying services' APIs if available, such as for Skype [16], or instrumenting their phone to take screenshots at regular intervals). Such automated observation of OSIs enables a scaled attack, whereby an adversary could concurrently collect OSI data for *many* users. Although 22 apps in our analysis had OSIs that were visible only to "friends" or contacts, prior work has shown that many users accept friend requests from strangers [30]. Thus, this risk is not limited to apps with globally viewable OSIs. Additionally, automated observations would enable an adversary targeting a *specific* person to collect and leverage longitudinal OSI data, which could more reliably expose patterns in the target's app usage than manual observations.

5.2 Best Practices

Our findings systematically characterize common design patterns in this space and therefore document themes that users are likely to encounter when engaging with OSIs. Here, we describe preliminary design recommendations based on the patterns we identify — which likely influence and inform user expectations about OSIs — coupled with prior work. Future work remains to empirically validate these recommendations with users.

Green Color Scheme. Over half of the apps we studied (21) already used green dots to indicate that a user was online. Prior work has documented that *external consistency* — that is, consistency across different experiences that perform similar functions [18] — improves users' performance and understanding [4]. Thus, there is theoretical justification for hypothesizing that the green dot design will more readily convey OSI functionality to a user. We encourage designers to reuse the green-dot pattern to indicate that a user is online, and future work could evaluate its efficacy with users.

Salient OSIs. In many apps, we found that OSIs appear in prominent places, such as in user profiles, news feeds, or lists of friends. Many apps display status changes with high salience as well, for example, notifying users proactively when someone comes online. This prominence has the potential to increase users' cognizance that their own online status is being shared, and prior work has shown that interface design can systematically influence users' public and private self-awareness [23, 25, 32]. Thus, designers may have levers at their disposal to increase or decrease users' awareness of what they disclose through their OSIs, and displaying online status in prominent locations and showing a user their own OSI removes the need for the user to imagine what others might observe.

Conservative Defaults. More restrictive audience defaults have the potential to help users avoid

OSI-related privacy violations. Our app analysis showed that nearly half of apps with OSIs expose a user's OSI information to *all* other users of the application by default. Prior work has shown that users consistently underestimate their audience when using social apps [7], suggesting that many people may be unaware of the breadth of their OSI audience. Other work has also suggested that presence information be made available only to contacts [10]; here, we show that it is common for apps to violate this recommendation. Apps could funnel users toward making a deliberate decision about whether to share their online status by: 1) providing more restrictive audience defaults, 2) turning online status off by default, and 3) actively prompting users to choose whether they prefer to appear online.

Provide OSI Settings. Designers should include a mechanism to turn off UI that automatically broadcasts online status. Approximately half of the apps in our analysis (19, plus Grindr's newly-added feature for paid users and Hearthstone's ability to change this via the Battle.net app) already do this. As recommended in prior research [20], OSI settings that let users specify whether OSIs are on for *specific* friends can give users additional control.

Undetectable Changes to Settings. In some of the apps we reviewed, an observer could detect when a user was truly offline versus when they had simply adjusted their settings to appear offline. By obscuring this difference and making it impossible for observers to detect whether someone has turned off OSIs, designers can better represent the user's intention of appearing unavailable.

No Reciprocity. Buchenscheit et al. found that participants were hesitant to turn off their own "last seen" indicators because they wanted to see others' [10]. We found that 10 of 19 apps with OSI settings enforce reciprocity, such that viewing another user's OSI requires displaying one's own.

While reciprocity of OSI settings could be seen as a nudge towards social connection, app-enforced reciprocity 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. We recommend that apps do not require reciprocal OSI sharing to see someone else's OSI.

Immediate online/offline updates. As discussed, low-level implementation details, such as how long it takes for users to appear online or offline after opening or closing an app, can affect an adversary's ability to monitor someone via their OSI. Although short update times create a more fine-grained record of a person's behavior, we 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 a user was actually online at any given time.

5.3 Design Concepts for Managing Presence

Since our taxonomy of OSIs covers a wide range of designs, we used the taxonomy to scaffold a brainstorming exercise within our research team focused on alternative OSI deigns that do not currently exist. Here, we present some designs that we think are especially promising.

Because of the randomness in the way that Tumblr displays OSIs (see Section 5.1), we could observe a user's online/offline behaviors only by repeatedly refreshing the app. This, and all of the implementations of OSIs that we observed, support the likely undesirable 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 shows users who accessed their OSIs 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 they could view someone's online status or leverage concepts from differential privacy research to limit the amount that any one person's online status could be viewed by others, providing theoretical guarantees about the inferences adversaries could make.

The apps we analyzed have three general "modes" for how OSIs might reflect online status: (1) accurately reflecting whether the user is online or offline, (2) causing the user to appear as though they were offline, or (3) showing some other static OSI such as that the user has turned off their OSI. Letting users choose a schedule for when they should or should not appear as online, letting users appear to be online at random intervals, or letting users continuously appear *online*, even while offline, would be interesting alternatives to explore. Notably, a third-party service or client-side program could approximate some of these functionalities without requiring buy-in from app developers (i.e., causing a user to appear online when desired, not necessarily related to them actually opening the app), which could be used to *always* appear as online.

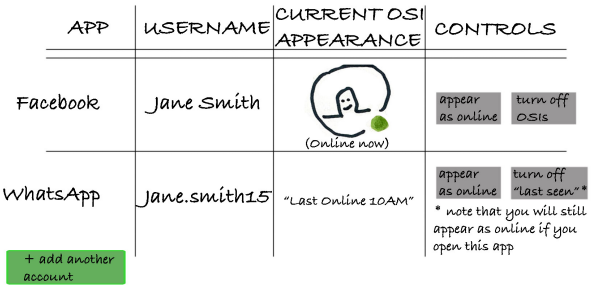

Fig. 12. We propose a third-party OSI manager to help users control OSIs for multiple apps or accounts using a unified interface.

The existence of OSIs that propagate between apps (e.g., Hearthstone and Battle.net) led us to consider the idea of a broader third-party OSI manager that enables users to manage OSIs across multiple apps and/or accounts from a single interface (Figure 12). This could reduce the cognitive load for users who interact with a variety of apps that have OSIs.

6 Conclusion

In this paper, we presented a systematic review of 184 mobile apps to identify the prevalence of online status indicators (OSIs) across the app ecosytem. We conducted a comprehensive design analysis of the 40 mobile apps with OSIs, which we used to generate a taxonomy of OSI features, with a particular focus on design aspects that affect users' ability to meet their privacy needs. We discuss how these thematic design decisions affect adversaries' ability to maliciously monitor and leverage OSI information, such as how accurately the OSIs reflect actual user behavior and users' ability to conceal their activity. We suggest best practices for improving user privacy within the existing design space of OSIs and offer novel design ideas for re-imagining OSIs that extend beyond the taxonomy of existing designs.

Acknowledgements

We thank Lujo Bauer, Ryan Calo, Dawn Cobb, Ivan Evtimov, Earlence Fernandes, Kiron Lebeck, Ted Mack, Franziska Roesner, John Toman, and Eric Zeng for providing help with and feedback on this work. We thank Kai Lukoff for sharing data from a previous study about participants' app usage. We would also like to thank our anonymous reviewers for their helpful feedback and our shepherd Kevin Huguenin. This research was supported in part by the University of Washington Tech Policy Lab, which receives support from: the William and Flora Hewlett Foundation, the John D. and Catherine T. MacArthur Foundation, Microsoft, the Pierre and Pamela Omidyar Fund at the Silicon Valley Community Foundation, and NSF Grant Number 1565252.

References

[1] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. Sok: Security evaluation of home-based IoT deployments. In *IEEE S&P*, 2019.

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

[3] Daniel Avrahami and Scott E. Hudson. Responsiveness in instant messaging: Predictive models supporting interpersonal communication. In *CHI*, 2006.

[4] Anton Axelsson. Consistency in web design from a user perspective. Bachelor thesis, 2012.

[5] James "Bo" Begole, Nicholas E. Matsakis, and John C. Tang. Lilsys: Sensing unavailability. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, CSCW '04, 2004.

[6] 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.

[7] Michael S. Bernstein, Eytan Bakshy, Moira Burke, and Brian Karrer. Quantifying the invisible audience in social networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, 2013.

[8] 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.

[9] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE S&P*, 2012.

[10] 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.

[11] Melissa N. Callaghan and Stephanie M. Reich. Are educational preschool apps designed to teach? An analysis of the app market. *Learning, Media and Technology*, 2018.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] Get a person and listen for availability. https://docs.microsoft.com/en-us/skype-sdk/websdk/docs/listenforavailability. Accessed: 2020-03-01.

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

[18] Jonathan Grudin. The case against user interface consistency. *Commun. ACM*, 32(10), October 1989.

[19] 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.

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

[21] Stacie Hibino and Audris Mockus. handimessenger: Awareness-enhanced universal communication for mobile users. In *Proceedings of the 4th International Symposium on Mobile Human-Computer Interaction*, Mobile HCI '02, 2002.

[22] Eric Horvitz, Paul Koch, Carl Myers Kadie, and Andy Jacobs. Coordinates: Probabilistic forecasting of presence and availability. *CoRR*, abs/1301.0573, 2013.

[23] Adam Joinson. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, 31, 03 2001.

[24] 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.

[25] Kimberly Matheson and Mark P. Zanna. Computer-mediated communications: The focus is on me. *Social Science Computer Review*, 8(1):1–12, 1990.

[26] 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.

[27] Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi M. Weeks, Yung-Ju Chang, and Jenny Radesky. Advertising in young children's apps: A content analysis. *Journal of Developmental & Behavioral Pediatrics*, 2018.

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

[29] National Coalition Against Domestic Violence Statistics. ncadv.org/statistics. Accessed: 2019-12-14.

[30] Hootan Rashtian, Yazan Boshmaf, Pooya Jaferian, and Konstantin Beznosov. To befriend or not? A model of friend request acceptance on Facebook. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014.

[31] Anne Spencer Ross, Xiaoyi Zhang, James Fogarty, and Jacob O. Wobbrock. Epidemiology as a framework for large-scale mobile application accessibility assessment. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '17, 2017.

[32] Young June Sah and Wei Peng. Effects of visual and linguistic anthropomorphic cues on social perception, self-awareness, and information disclosure in a health website. *Computers in Human Behavior*, 45, 04 2015.

[33] Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, and Matthew Smith. Sok: Secure messaging. In *IEEE S&P*, 2015.

[34] XMPP — Wikipedia. https://en.wikipedia.org/wiki/XMPP. Accessed: 2020-02-03.

A Appendix A: Apps Identified for Analysis

We identified 184 apps for analysis based on several inclusion criteria (see Section 3), designed to include popular apps from a variety of app genres and target audiences, with an intentional bias toward apps that have OSIs. All 184 apps are listed in Table 3.

B Appendix B: Screenshots of OSIs in All 40 Apps with OSIs

Although many of the OSI characteristics we describe in this paper cannot be captured in a single screenshot, we include screenshots from all 40 apps with OSIs to capture the wide range of OSI icon designs in this set. Screenshots have been altered to remove account data.

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	Uber Eats	Android Auto	Duall	Chase Mobile	**Battle.net**
Audiobooks from Audible	DoorDash	Baseball Boy	Flickr	Dropbox	Bumble
Bible	McDonald's	Color Road	Flipkart	eBay	Candy Crush
Amazon Kindle	Grubhub (2)	DHgate-Shop	Gmail (3)	Google Calendar	Canvas (student portal)
Libby, by OverDrive	Domino's Pizza USA	Draw In	**(Google) Hangouts (3)**	Google Drive	CareZone
Communication	Medical	Episode -- Choose your story	Google Plus	Google Docs or Google Sheets	Castlight Mobile
(Facebook) Messenger (1,2,3)	Family 5 & Under	Flip the Gun	Google Voice (3)	Google Keep	eharmony Dating
WhatsApp Messenger (1, 2, 3)	YouTube Kids	Flying Arrow	**Grindr**	Google Opinion Rewards	Facebook Local
(Facebook) Messenger Lite (1)	(also in all other Family categories)	Granny	**Hike**	Google Play Music	Fitbit
Marco Polo Video Walkie Talkie	Toca Kitchen 2 (also in Family 6-8)	Helix Jump	**imo**	Imgur	Glow Baby
Yahoo Mail	PBS Kids Games	**Jurassic World Alive**	Kik	Lookout Security & Antivirus	Goodreads
Dating	PJ Masks: Moonlight Heroes	Kick the Buddy	Line	Lyft	GroupMe
Zoosk Dating	Family 6-8	LetGo	**LinkedIn**	(Google) Maps	**Happn**
Match Dating	Pandora (1, 3)	Love Balls	Mindmeister	Nova Launcher	**Hearthstone**
CoffeeMeetsBagel Dating	Spotify (1, 2, 3)	News Break: Local	MyRadar	OneBusAway	Hinge Dating
OkCupid Dating (2)	**(Facebook) Messenger Kids (also in Family, overall)**	**OfferUP**	Reddit	reddit is fun (unofficial)	iHeartRadio
JOYRIDE Dating	Free Music Plus (1)	Partymasters	Signal	Robinhood	Indeed
Education	SoundCloud	Pixel Art: Color by Number Game	**Skype**	Slack	Insight Timer
Duolingo	YouTube Music	**PUBG MOBILE**	Surfline	Starbucks	Memrise
ABCmouse.com (also in Family 5 & Under)	Social (Top 10)	Rise up	**Telegram**	Swagbucks	Nextdoor
Language Translator: easy, free, efficient	Snapchat (1, 2, 3)	Run Sausage Run	Tinder (3)	T-Mobile Tuesdays	**Steam**
Lumosity	**Instagram (1, 2, 3)**	Sling Drift	Topbuzz	Textra SMS	Strava
Remind: School Communication	**Facebook (1, 2, 3)**	slither.io	**Tumblr (3)**	**Waze**	Whisper
Entertainment	musical.ly (1, 2)	Snake VS Block	**Twitch**	Yelp	**Words with Friends**
Netflix (1,3)	TextNow (1)	Subway Surfers	Twitter (3)		Yousician
Bitmoji (1)	FindNow	The Cube	UC Browser		**Yubo**
Google Play Games (1)	Messages, Text and Video Chat for Messenger (NOT Facebook)	Toon Blast	**Viber**		
Hulu (1)	Pinterest (2, 3)	Uber (3)	WeChat		
Amazon Prime Video (1)	**Facebook Lite**	Will it Crush?	YouTube (3)		
	POF (Plenty of Fish) Dating	Wish			
		Word Link			

grey text - no social features
bold - has *typical* online status indicators
blue - (typical) online status can be turned off
(1) App is also in Top 50 Apps

normal black text - has social features (but not OSIs)
Underline - has *sub-area* online status
red - (typical) online status cannot be turned off
(2) App is also in Novice Suggestions

(3)App is also in real app usage data

Table 3. The 184 apps included in analysis, sorted by inclusion criteria. Numbers next to apps indicate that they fall within multiple inclusion criteria. Apps are shown with different font color and style based on high-level findings, such as whether they have social features or OSIs.

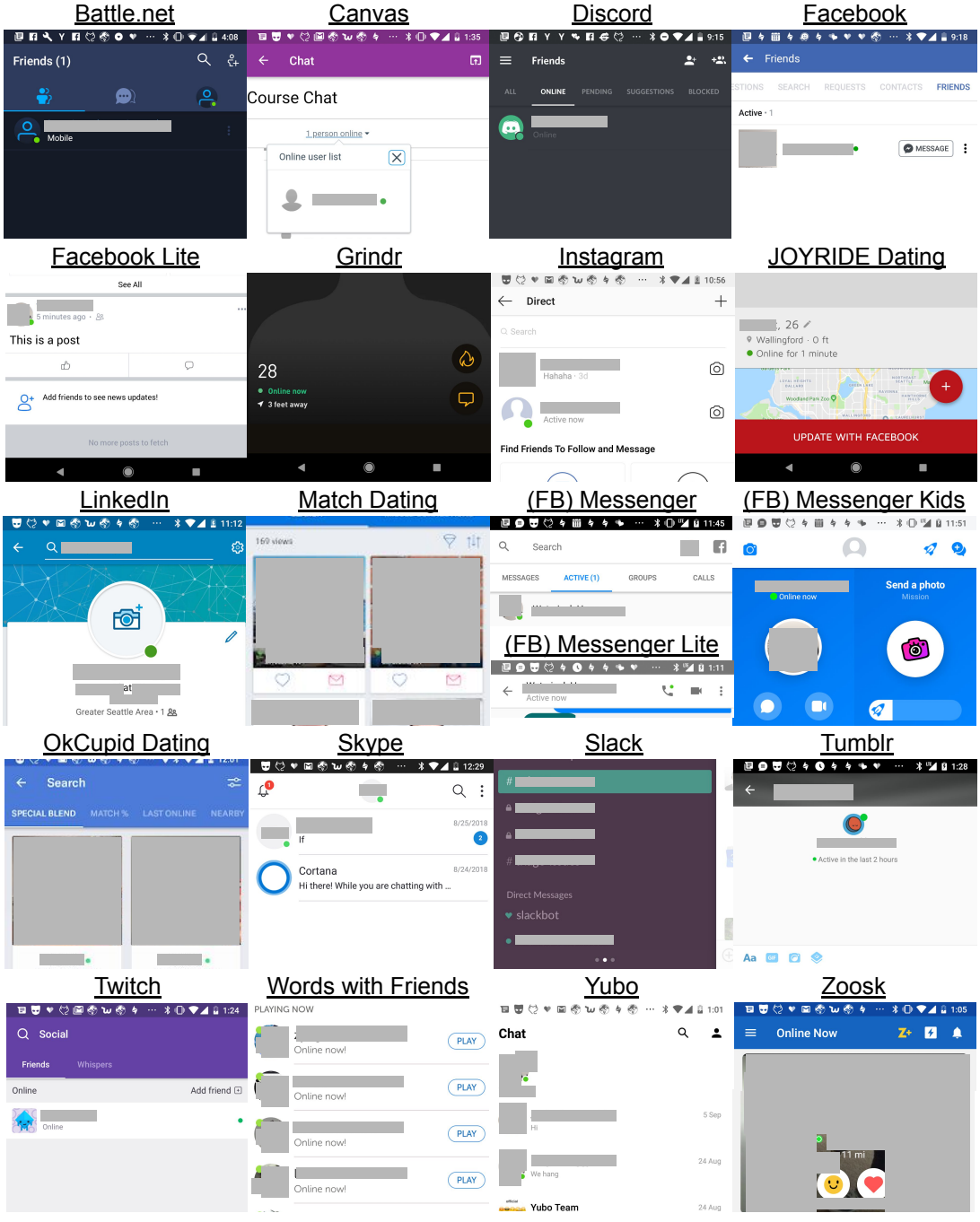

Fig. 13. Screenshots of apps with green dot OSIs, shown alphabetically. Many of these OSIs also include text or other OSI features to convey redundant or additional information.

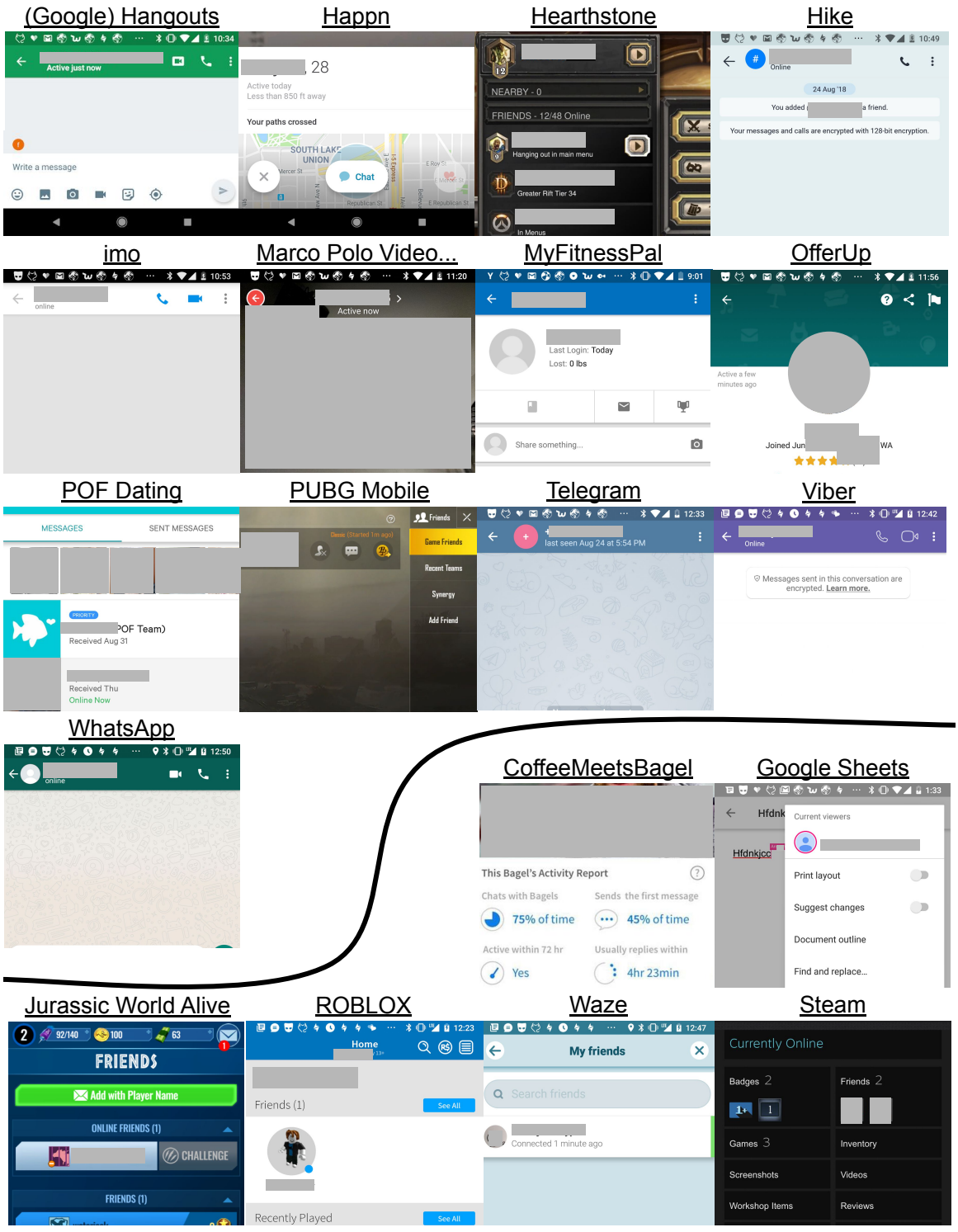

Fig. 14. Screenshots of apps with OSIs that are not green dots, separated into two groups: those with a text-only OSI (above the line) and those with an icon that is not a green dot (below the line). For apps with text-only OSIs, the exact text can vary in content and color. Some apps, such as Hearthstone, convey more information than simply *whether* a user is online.