User Experiences with Online Status Indicators

Camille Cobb
Carnegie Mellon University
Pittsburgh, PA
ccobb@andrew.cmu.edu

Lucy Simko
University of Washington
Seattle, WA
simkol@cs.washington.edu

Tadayoshi Kohno
University of Washington
Seattle, WA
yoshi@cs.washinton.edu

Alexis Hiniker
University of Washington
Seattle, WA
alexisr@uw.edu

ABSTRACT

Online status indicators (OSIs) improve online communication by helping users convey and assess availability, but they also let users infer potentially sensitive information about one another. We surveyed 200 smartphone users to understand the extent to which users are aware of information shared via OSIs and the extent to which this shapes their behavior. Despite familiarity with OSIs, participants misunderstand many aspects of OSIs, and they describe carefully curating and seeking to control their self-presentation via OSIs. Some users further report leveraging OSI-conveyed information for problematic and malicious purposes. Drawing on existing constructs of *app dependence* (i.e., when users contort their behavior to meet an app's demands) and *app enablement* (i.e., when apps enable users to engage in behaviors they feel good about), we demonstrate that current OSI design patterns promote app dependence, and we call for a shift toward OSI designs that are more enabling for users.

Author Keywords

Privacy; Mobile Apps; Online Status; Social Computing

CCS Concepts

•Security and privacy → Social aspects of security and privacy; Usability in security and privacy; •Human-centered computing → *Social content sharing;* Smartphones;

INTRODUCTION

Online Status Indicators (OSIs) are UI elements that broadcast whether a user is or was recently online, updating automatically as a user comes and goes [11]. Unlike the information that users intentionally and consciously share — such as posts, profile updates, or messages — OSIs project users' behaviors to others without explicit direction from the user and in a way that is often not easily controlled.

This unsolicited sharing has the potential to expose the user to privacy risks. Prior work has shown, for example, that OSIs in WhatsApp can reveal insights about someone's daily routines, such as sleep and wake times, and who they communicate with [9]. Other work has shown that "read receipts," another UI mechanism that passively shares information about user behavior, inadvertently reveal sensitive information that users may prefer not to disclose [24]. These findings hint that across experiences, OSIs in general may create systematic privacy concerns through the status information they share.

OSIs are increasingly common and are present in many of the most popular social and communication apps [11]. A number of studies have investigated the potential for OSIs to improve users' ability to connect and coordinate with one another [1, 34]. However, their risks have not yet been systematically investigated across apps, despite suggestions that such risks exist. Developing a more robust understanding of the impact of passively broadcasting users' status promises to help the research community better advocate for consumers. Thus, we asked:

1. To what extent are users exposed to OSIs, and what are the characteristics of the OSIs they encounter?
2. What are users' mental models of what is shared and when by OSIs?
3. How do OSIs influence user behavior? What are users' privacy-related preferences and experiences with OSIs?

To investigate these questions, we deployed an online survey to 200 workers on Amazon Mechanical Turk to explore users' knowledge about and experience with OSIs in mobile applications. We report on participants' exposure to specific apps with OSIs, interpretation of information conveyed by OSIs, awareness of OSIs in the apps they use, ability to locate settings to change the behavior of OSIs in the apps they use, and descriptions of their experiences using OSIs. In addition to characterizing users' experiences with OSIs broadly, we examine how specific design decisions (such as the color of an OSI icon, or the ability for a user to see others' OSI icons after turning off their own) affect users' ability to anticipate and control their privacy as it relates to OSIs.

CHI '20, April 25–30, 2020, Honolulu, HI, USA.
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
https://doi.org/10.1145/3313831.3376240

We found that participants readily recognized common OSI design patterns, but they held many uncertain or incorrect beliefs about their functionality. They were often mindful of the information their own OSIs might convey to others, and many reported altering their own behavior as a result. Drawing on existing constructs of *app enablement* and *app dependence* [16], we show how current OSI designs prompt users to contort their behaviors to manage their OSI display, leading to app dependence (i.e., behaviors dictated by the app rather than the user's intrinsic needs and desires).

We also found that participants both notice and make inferences about other people's online status, sometimes reacting to it in potentially problematic ways (e.g., surveilling intimate partners). We provide guidance for designing OSIs that better support users' privacy goals.

RELATED WORK

Understanding and Designing OSIs

A number of studies have examined users' experiences with OSIs and their precursors. Nardi et al. studied 20 participants' experiences with early Instant Messaging (IM) tools in a workplace setting and found that "*awareness information about the presence of others*" (i.e., OSIs) provided a variety of benefits to users [34], including enabling them to negotiate when they were available to other colleagues. However, in doing so, participants sometimes leveraged the imprecision of these early tools to provide plausible deniability about whether they were actually online or offline. This cover allowed employees to be available to others on their own terms. More recent work has found that, in contrast, modern OSIs in some mobile apps reflect actual online/offline behavior very accurately, thus providing more precise information but potentially compromising users' ability to manage interpersonal relationships [11].

As these UI elements have evolved in the intervening years to become a mainstream part of many apps and websites, a substantial amount of work has continued to explore the design of OSIs. One direction of inquiry has investigated leveraging patterns in users' presence data to predict and convey to others whether someone is truly available to talk or simply online [1, 2, 22, 23]. De Guzman et al. explored novel OSI designs, including standalone light fixtures and sounds from a wind chime to indicate that a friend was online [14].

OSIs and Privacy Concerns

Early OSIs often used video of a physical space to determine if a user was online, and in some instances, even reflected these videos back to others as their mechanism of showing someone's availability [7, 18]. Although these early privacy-invasive designs are not widely circulated, there is substantial evidence that modern OSIs still present privacy risks to users. OSIs now extend beyond the workplace and are more ubiquitously deployed in services accessed on mobile devices rather than only in a constrained desktop environment.

Other work has shown that online status information can be used to infer more specific, potentially sensitive, details about a user. For example, OSIs can reveal users' daily habits, when they deviate from typical habits, if they are using apps when they should not be (e.g., while at work), their physical location, and which other users they are conversing with [3, 8, 9, 15]. In a study of OSIs on WhatsApp, Buchenscheit et al. found that participants were observant of their friends' OSIs and made inferences about their behaviors (e.g., inferring how late someone stayed a party) [9]. And these concerns may be exacerbated in certain contexts; in a study of undocumented immigrants' privacy concerns, Guberek et al. mention one participant's observation that her former partner could use OSIs in WhatsApp to keep track of her [19]. In our work, we build on these studies, taking a broader view of how OSIs can affect users' privacy; in particular, we explore users' experiences with a variety of apps that have OSIs and consider not just what information is reliably leaked but also how users make inferences about their friends' OSIs that go beyond what could be inferred from the data alone.

Presentation of Self Online

A vast amount of prior work has explored the ways that people manage their online self-presentation. Users of all ages and backgrounds work to curate their online image and manage the impressions they give to others in networked spaces. People share location-based check-ins as a way to achieve social aims [20], adults curate their online histories to selectively redact digital traces from their adolescence [35], and transgender users who transition often remove pre-transition photos from online spaces as a component of updating the identity they project [10].

According to Goffman, people seek to manage in-person impressions based on context and audience [17]. 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 [4, 6, 13, 25, 27, 37, 40]. Understanding and managing the audience for online self-presentation can be especially difficult. Research has found, for example, that people consistently underestimate the size of their audience [5]. A related obstacle that interferes with users' success at managing their privacy is "context collapse" [32, 33, 39]. Prior work has examined some strategies and techniques that people develop for managing and limiting the audience of content they post online, such as thoughtfully considering who to add as friends, maintaining multiple online profiles with differing audiences, self-censoring [38].

Privacy Settings and Adjusting Audience

As discussed by Vitak et al. [38], one way users can manage their online privacy is via privacy settings provided by an app or service. However, researchers within the usable security and privacy community have repeatedly found that these settings are inadequate.

In some cases, users' expectations of privacy do not match reality due to user misunderstanding or mis-configuration of privacy settings [29, 30, 36]. For example, Liu et al. found that in most cases where users have updated settings on Facebook, the modified settings do not match their expectations [29].

Despite research that seeks to improve the ability for users to successfully understand and use these settings (e.g., finding that showing users an audience-oriented view of their profile helps them understand privacy settings [28]), users' inability to reason about their own privacy settings may not be the only barrier to achieving privacy goals. Prior work has found that the choices apps offer in some cases do not allow users to simultaneously accomplish their privacy goals *and* other goals for using a service [12, 26]. For example, Johnson et al. found that most users could protect against unintended disclosure to strangers on Facebook, but that the settings were inadequate for managing the *insider threat* of unintended disclosure to Friends. In this paper, we find, similarly, that users have both misunderstandings about OSI settings and are not sufficiently supported by them.

METHOD

Participants

We recruited 205 people on Amazon Mechanical Turk to participate in an online survey, approved by our institution's IRB. Participants were disproportionately white, well-educated, and from the United States (see Table 1). All participants had previously completed at least 1000 HITs with a 98% acceptance rate. We excluded four participants, because their answers suggested that they did not understand the survey and one person who submitted the survey twice. Thus, our final data set included 200 complete survey responses. We paid participants a base rate of US$3, in addition to the bonuses specified below.

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 1. Summary of survey participant demographics

Survey Design and Procedures

We designed a five-part survey to evaluate users' mental models of OSIs and explore their experiences with these features. Questions were asked in this order, and participants could not go back to previous survey pages. Survey sections included:

1. A checklist of apps with OSIs and a question asking participants which of these apps they use regularly
2. A randomized experiment evaluating the salience of five common OSI design patterns
3. A questionnaire evaluating participants' understanding of the OSIs in the specific apps they use
4. A task evaluating participants' ability to locate OSI settings in the apps they use
5. A series of open-ended questions probing participants' experiences with and attitudes toward OSIs

We describe each of these sections in more detail below. On average, the entire survey took 22.56 minutes to complete (sd = 18.30 minutes).

Survey Section 1: Exposure to OSIs

Recent prior work identifies a broad set of apps with OSIs, extracted through a systematic review of commercially available mobile applications for the Android and iOS operating systems [11]. This review identified apps by both popularity and breadth, leading to a diverse and comprehensive set of 40 mobile apps with OSIs. We used this set as the basis for a checklist of apps to probe our participants' exposure to OSIs. We intentionally excluded "Facebook Messenger Kids," as all participants were adults, and we inadvertently left off the "Joyride Dating" online dating app, leaving us with 38 entries. To understand where and how often users are exposed to OSIs, we presented this list of 38 apps to participants and asked them to select each app on the list they use at least once per week.

Survey Section 2: Recognizing OSI Design Patterns

We then performed an experiment to evaluate how OSI design patterns (e.g., dot icons, text labels, color) affect recognition and understanding of OSIs. Each participant saw a series of five images (Figure 1), each depicting an OSI. Each new image was displayed in isolation (only one image at a time).

Each image layered on additional UI that depicted a common OSI design pattern. Participants saw the OSI in one of four randomly assigned colors: green (N = 50), orange (N = 41), blue (N = 53), or grayscale (N = 56). In this final group, grayscale was applied to the entire image, acting as a control by eliminating all color information. This experimental design allowed us to make within-subjects comparisons of how additional UI affected users' recognition of OSIs and between-subjects comparisons of how OSI icon color affected users' recognition of OSIs. Importantly, this does not reflect all OSI design patterns that could affect users' understanding of OSIs, such as the shape of the OSI icon or using other text to indicate that someone is online (e.g., "Active Now" rather than "Online Now").

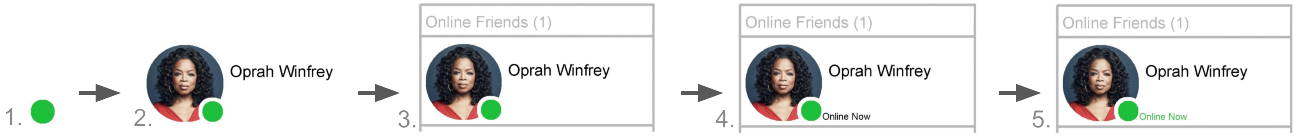
For each image, participants provided an open-ended response describing what they thought the dot was (Figure 1, bottom). After the full progression of images, we asked participants to assess whether "Oprah Winfrey" (whose name and photo appeared in the images they saw) was currently using the app based on the final image. Participants were given a chance to submit open-ended comments describing their thought process as they had answered the previous questions.

Survey Section 3: App-Specific OSI Knowledge

For each app a participant reported using regularly in Survey Section 1, we asked them to tell us, without looking at their phone, whether they believe it has OSIs. To ensure all participants understood what an OSI was, we provided a description and showed the examples (Figure 2) before this question.

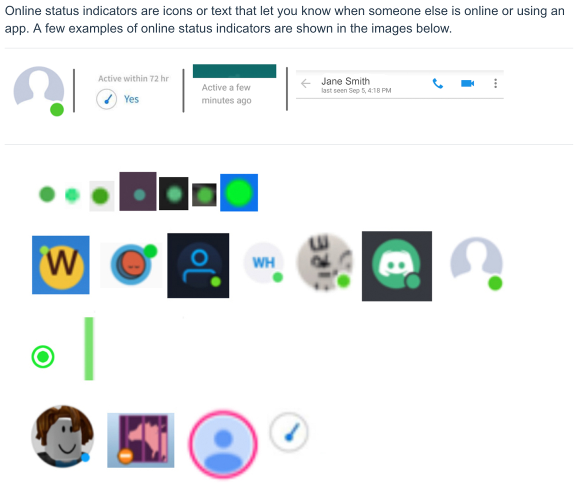
Survey Section 4: Locating OSI Settings

Once again iterating through each app the participant reported using regularly, we asked the participant to open the app on their phone and time themselves to see how long it took to find OSI settings. Specifically we asked them to, "find the settings



If you opened an app and saw a dot like the one in the image above, what would you think the dot means? (That is, what information is the dot meant to convey?)

Figure 1. In the experimental component of our 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.



Online status indicators are icons or text that let you know when someone else is online or using an app. A few examples of online status indicators are shown in the images below.

Figure 2. This image and explanation were shown to participants to minimize the possible impacts of which experimental condition they experienced in the previous section of the survey.

to turn off online status (that is, settings to make yourself appear offline to other users, even when you have the app open)." We did not ask participants to change their settings, only to find them. Participants received a US$0.50 bonus for each app they reported timing. Participants could enter free-response comments about the process of looking for settings. We conservatively excluded all timing data reported by 33 participants whose answers or free-response explanations suggested they may not have actually completed the task.

Survey Section 5: Users' Experiences with OSIs

Finally, we asked participants to describe their experiences with OSIs. For each of five unique OSI-related scenarios, we asked participants to both: 1) say whether the scenario described an experience they have had with OSIs, and 2) optionally describe a personal experience relating to the scenario. These five prompts were:

- *Is there anyone who would notice if you were offline for longer than usual (i.e., based on your online status indicator), or are there any people for whom you would notice if they were offline for longer than usual?*
- *Have you ever been surprised to notice that someone was online (i.e., based on their online status indicators)?*
- *Have you ever opened an app specifically to check if someone was online (i.e., look at their online status indicators)?*
- *Have you ever suspected that someone noticed that you were online (i.e., noticed your online status indicator)?*
- *Have you ever changed your behavior (e.g., avoided opening an app) because you didn't want to appear as "online" (i.e., have your online status indicator show that you are online)?*

To generate these prompts, we conducted a design exercise with 17 university-affiliated security and privacy experts during a regularly occurring 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 affinity diagramming. One representative from the panel worked with research team to translate these clusters into the five survey prompts above.

At the end of this section, we included one additional chance for participants to "describe any other noteworthy experiences" they had with OSIs. We paid a bonus up to $2 for answering free-response questions. At the end of the survey, we collected demographic information.

Data Analysis

A single researcher first made determinations about excluding data, which were informed by conversations with the other researchers, but the other researchers did not look at the data at this stage to help make this decision.

Next, we analyzed the open-text responses for the experimental component of the survey, asking participants what the dot meant in an image of an OSI, which we wanted to use for quantitative analysis. One researcher coded all responses to determine if participants had correctly determined that the dot was an OSI. A secondary coder coded 10% of the responses to determine inter-rater reliability and saw a high degree of agreement (Cohen's k = .94). We coded participants' responses as correct if they identified that the dot meant that the person was online or available. We coded responses as partially correct if participants offered multiple possible explanations for the meaning of the dot, or if they understood that the dot was an OSI but believed that it indicated that the person was *not* currently online.

We analyzed all remaining open-ended qualitative data using an inductive-deductive approach. This included participants' responses about: (1) their thought processes during the experiment, (2) their experience looking for OSI settings, and (3) the open-ended questions about their experiences with OSIs. Two researchers independently identified themes through open coding within each of the aforementioned three sets of qualitative data. We then collaboratively discussed these initial themes and defined a set of axial codes. Using these refined definitions, one researcher iteratively coded all responses.

RESULTS

Exposure to OSIs in Mobile Apps

To understand the extent to which users are exposed to OSIs, and the types of OSIs they see most often, we first examined the frequency with which users engaged with the pre-selected 38 apps with OSIs (see Table 2). Of all participants, 99% regularly used at least one app with OSIs, and on average, participants regularly used 5.11 apps with OSIs (sd = 3.04, median = 4, max = 15).

Instagram and Facebook were the most commonly used apps, regularly used by over half of participants. An additional five apps were used by at least 25% of participants. Thus, participants had been broadly and routinely exposed to the OSI-related design decisions embedded in these seven apps.

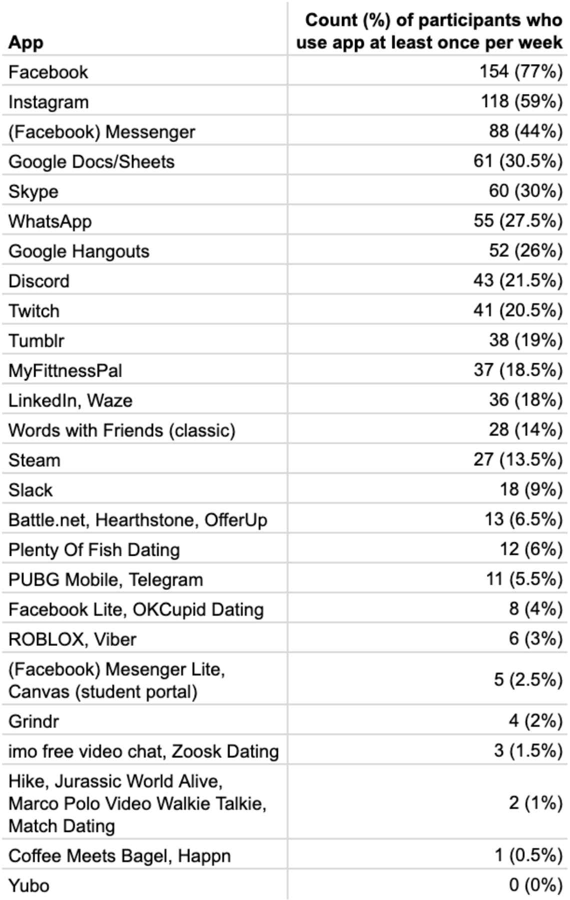
Comparing against an existing technical analysis that characterizes the design of OSIs in the 38 apps we presented [11], we linked the design features of specific apps to participants' use, enabling us to document the extent to which participants are exposed to specific design decisions (see Table 3). For example, although only half of the 38 listed apps provide settings to turn off OSIs (i.e., allow the user to stealthily use the app while still appearing offline), 97.5% of participants regularly use at least one app with this feature.

Participants were almost universally exposed to a few other patterns. For example, 98.5% of participants used at least one app that reveals their OSI only to users with whom they are explicitly connected (e.g., as friends or contacts). Separately, 94.5% used at least one app in which disabling one's own OSI prevents that user from seeing others' OSIs. And 96.5% of participants used at least one app that represents online status with a round, green dot. Although these usage habits alone do not reveal the extent to which users notice these patterns, they reveal a number of OSI designs that are distributed widely.

Recognition of OSI Design Patterns

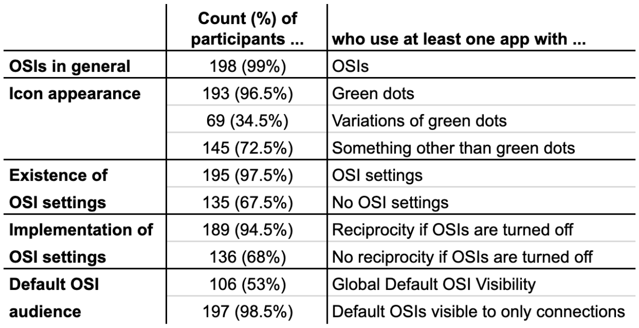
The results of the experimental component of our study designed to evaluate users' recognition of OSI design patterns (Figure 1) are shown in Figure 3. As each participant saw a dot of a single color surrounded by progressively overt visual cues indicating the dot represents an OSI, we first evaluated, for each person and for each cue, whether the participant accurately understood the purpose of the UI as an OSI. We calculated a cue-number score for each participant – 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 ($F(3,160) = 12.640$, $p < .001$, $\eta^2 = .192$). *Post hoc* analysis revealed that participants who saw a green dot



App	Count (%) of participants who use app at least once per week
Facebook	154 (77%)
Instagram	118 (59%)
(Facebook) Messenger	88 (44%)
Google Docs/Sheets	61 (30.5%)
Skype	60 (30%)
WhatsApp	55 (27.5%)
Google Hangouts	52 (26%)
Discord	43 (21.5%)
Twitch	41 (20.5%)
Tumblr	38 (19%)
MyFittnessPal	37 (18.5%)
LinkedIn, Waze	36 (18%)
Words with Friends (classic)	28 (14%)
Steam	27 (13.5%)
Slack	18 (9%)
Battle.net, Hearthstone, OfferUp	13 (6.5%)
Plenty Of Fish Dating	12 (6%)
PUBG Mobile, Telegram	11 (5.5%)
Facebook Lite, OKCupid Dating	8 (4%)
ROBLOX, Viber	6 (3%)
(Facebook) Mesenger Lite, Canvas (student portal)	5 (2.5%)
Grindr	4 (2%)
imo free video chat, Zoosk Dating	3 (1.5%)
Hike, Jurassic World Alive, Marco Polo Video Walkie Talkie, Match Dating	2 (1%)
Coffee Meets Bagel, Happn	1 (0.5%)
Yubo	0 (0%)

Table 2. The number of participants who reported that they regularly use each app in our survey. All of these apps have OSIs.



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

Table 3. Percent and number of participants exposed to varied design patterns identified in prior work [11], 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.

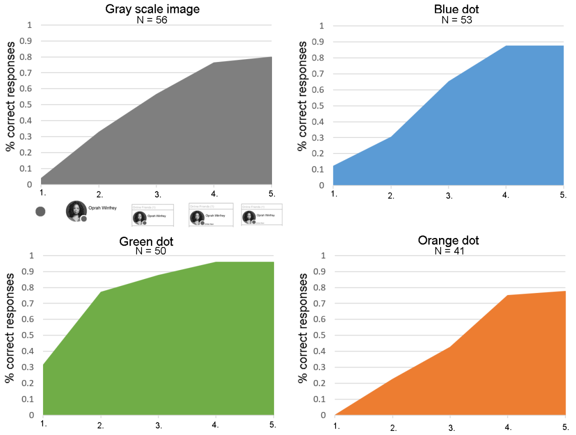


Figure 3. Results of the experimental component of our survey, which demonstrate that participants are more likely to recognize green dots being used as OSIs and that contextual cues helped them understand OSI icons even if the icon was a less typical color.

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. Additional statistical context, including effect sizes and confidence intervals, is shown in Table 4.

We next examined the cumulative impact of each of the visual cues we provided (i.e., the five progressive images in Figure 1 and on the x-axis of the gray graph in Figure 3). 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 ($Q(4) = 398.9$, $p < .001$). *Post hoc* comparisons revealed a significant jump in participant understanding between each pair of successive levels, except for levels 4 and 5, where we 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.

App-Specific OSI Knowledge

Almost all participants (198 of 200) reported regular use of at least one of the apps we 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 4 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.

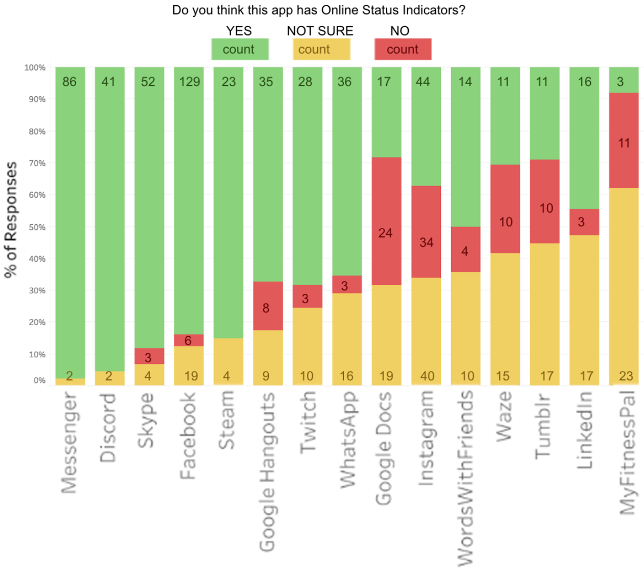


Figure 4. For apps used by at least 10% of participants, this graph shows what percent of respondents believed that the app did or did not have OSIs. For 10 of the 15 apps shown in this figure, more than 30% of participants did not answer correctly that the app has OSIs.

Locating OSI Settings

We asked participants to open each app they used regularly and find the settings options that would let them adjust their OSI. Although all apps did have OSIs, not all provided settings to adjust them, so participants could also specify if they believed that an app did not have settings or were unable to find the settings. Participants timed themselves conducting this task, and we obtained 683 timing reports from 154 unique users representing 35 apps.

- Participants reported locating these settings in the majority of cases (64% of all reports; 72% of reports for apps with OSI settings).
- Out of 524 reports for apps with OSI settings, 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 participants were particularly likely to be misled into thinking they had found an option for turning off their OSI. WhatsApp includes a setting to turn off "last seen" which prevents the

Condition 1	Condition 2	Mean Difference (C1 - C2)	SE	DF	*t*	*p*	95% CI
Green	Blue	-.81	.20	87	-4.05	.001	-1.35, -0.27
Green	Gray	-.93	.20	88	-4.67	< .001	-1.47, -0.39
Green	Orange	-1.24	.22	75	-5.92	< .001	-1.83, -0.65

Table 4. Statistical comparisons between the experimental conditions with green dot OSI icons and blue, gray and orange OSI icons.

app from showing *what time* someone was last online, but does not prevent the app from showing *whether* someone is online.

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."* 40 participants expected 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).

Experiences with OSIs

Several themes emerged through users' stories about their experiences with OSIs. Here, we describe three common themes that cut across the prompts we 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:

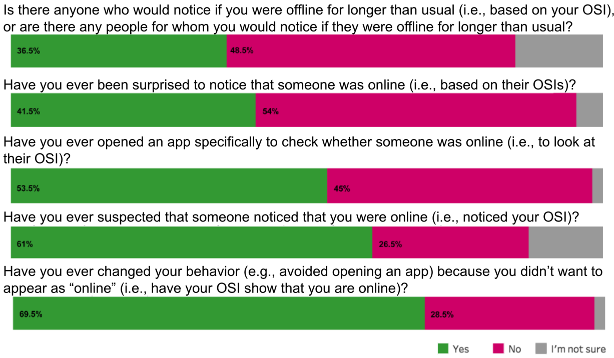


Figure 5. Through an expert panel of security and privacy experts, we developed 5 prompts to inquire about participants' experiences with OSIs. For each prompt, at least 35% of participants expressed that they had this experience.

> "[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."

Note that P27 was not alone in his particular focus on how a (former) romantic partner perceived his OSI. Many other stories participants conveyed centered on current or former romantic partners or romantic interests.

Three participants deleted an app from their phone altogether specifically to avoid appearing online. That so many participants reported using apps in non-preferred ways (occasionally abandoning the app altogether) points to a failure for apps to robustly support users' privacy preferences.

Participants 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 the observation from Cobb's taxonomy of OSIs that "cross-app OSIs" (i.e., OSIs that reflect whether a user is online to users in that app *and* other, related apps) may make it especially difficult for users to anticipate how they appear [11]:

> "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 Cobb identified in her analysis that support the ability for users to hide their OSIs from specific other users were Telegram and Hike [11] (used by only 11 and 2 participants, respectively), participants who expressed this preference likely found that the apps did not support this goal.

We 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."

This story illustrates a theme of users feeling 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. Or they say 'where have you been' like I've ARRIVED somewhere, when I really just opened my account."

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 well-being.

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 potentially harmful situations such as (perceptions of) "tracking" or being "tracked" via

OSIs, and confrontations stemming from observations of OSIs. For example, 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."

DISCUSSION AND DESIGN RECOMMENDATIONS

OSIs: Leaving Users App Dependent

Participants frequently misunderstood what their OSIs broadcast about them and when. Their descriptions reflected misunderstandings about the interface and uncertainty about their audience, which is consistent with prior work on context collapse [32, 33, 39]. 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 [16]. In this study, we found that current OSI designs frequently leave users app dependent, and we 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 [17]. Knowing this, designers can either support this image management or lead users to contort their activities to produce the desired OSI presentation.

OSIs as an Aspect of Social Surveillance

Most participants in our study described experiences with OSIs that involved their friends, family, or colleagues rather than strangers. People who know each other may be able to make informed inferences based on socially-gained knowledge, for example using OSIs to catch someone in a lie (or being caught in a lie because of appearing online), as participants discussed in our survey. However, participants also discussed many beneficial uses of OSIs — instances when they *did* want to share their OSIs with others or used someone else's OSIs to make inferences that were beneficial to the other person. For example, participants described looking to OSIs to avoid waking up or bothering their loved ones or checking that someone was safe. It would not be useful to discuss only the drawbacks of OSIs outside of this context.

In 2012, Marwick conceptualized users' mutual observations of people they know on social media as "social surveillance" and characterized the ways that social surveillance differs from traditional surveillance and how social surveillance influences users to carefully curate their online self-presentation [31]. Marwick discusses social surveillance as it relates to the content that appears on users' profiles (e.g., what they posted or friends' comments), and related work has also studied how users leverage location check-ins to manage impressions [20]. Our findings contribute to this research space, and we demonstrate that this online image management extends beyond intentionally posted social media content to include OSIs, which create a self-presentation as a byproduct of mere app use.

Design Considerations

Here we provide suggestions for how designers could support the user values and preferences related to OSIs that we identified in this work.

Appropriate Awareness of OSIs

We found that participants were significantly better at recognizing green dots as OSIs than they were at recognizing other colored dots. Further, we found that redundant contextual cues such as text that directly states "online now" or users being listed within a list of "online friends" also contributed to a better understanding of what these icons conveyed. Thus, designs that represent online status with a green dot are more likely to create an interface that is consistent with users' expectations, and text-based explanations that explicitly describe what is conveyed through an OSI provide cognitive shortcuts for users that support their understanding.

Users discussed the beneficial uses of OSIs, beyond communication-related benefits identified in previous work [1, 2, 3, 14, 22, 23, 34], such as being able to infer that their loved ones were safe. User stories that specified which apps participants wanted OSIs in coincided with the apps that they more frequently knew had OSIs. We gently suggest that perhaps some apps do not need to have OSIs. If most users are not aware that a beneficial but privacy-invasive feature exists, then this certainly tips the balance toward less benefit despite having the same privacy risk. Instagram's approach to OSIs, which shows OSIs only between users who have exchanged direct messages, may accomplish this aim. Although many participants did not realize Instagram had OSIs, users who do not use messaging do not *need* to know whether it has OSIs because no one will see their OSI.

Improving OSI Settings

Participants reported 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.

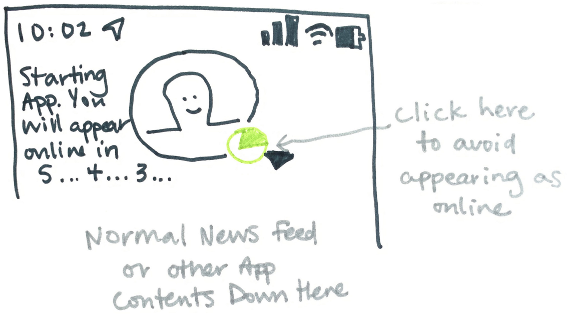

10:02
Starting App. You will appear online in 5...4...3...
Click here to avoid appearing as online
Normal News feed or other App Contents Down Here

Figure 6. Illustration of a design recommendations to let users turn off their OSI as they *open* an app.

Unfortunately, users expressed contradictory beliefs about their preferences for OSI settings designs — some expected to find OSI settings within the privacy menus while others thought that settings were "burried" if they were in these menus. Perhaps designers could allow OSI settings to be reached in multiple of the most commonly preferred ways.

One mistaken assumption participants made about OSI settings was related to how those settings propagate between apps that are logged into the same account (e.g., Facebook and Facebook Messenger). Several participants mistakenly thought that when they turned off their OSI in Facebook Messenger, it would also prevent them from appearing online on Facebook. We encourage designers to consider other ways to make the propagation (or lack thereof) more intuitive and/or privacy-preserving.

Enabling New OSI Controls

Eighty-five participants discussed a desire avoid specific other people seeing that they were online. Echoing a recommendation from prior research [21], we note that users may prefer to restrict the visibility of their online status to smaller audiences or to individually control which of their friends or contacts can see when they are online. According to Cobb's taxonomy of OSIs, most apps with OSIs do not currently provide this feature [11].

Even in apps that provide some kind of OSI settings, users may still not be able to control their OSIs in the ways they want. Participants in our study sometimes avoided opening an app because they did not want to appear online even long enough to change their OSI settings or did not change their behavior and subsequently felt that the OSI had "blown [their] cover" (P57). These concerns may be exacerbated for users seeking to avoid a specific other user, since they cannot know before opening an app themselves whether that other user is currently online. We propose that when users open an app, they could be given a grace period during which they do not appear as online. Apps could then provide an interface to allow users to avoid appearing online, as illustrated in Figure 6.

P45's feeling that their online friends behaved "like I've ARRIVED" when they came online conveys that some people see OSIs as analogous to entering a physical space (while others do not). The concept of "sub-area OSIs" (i.e., OSIs visible only between people mutually accessing some sub-area of an app, such as a one-on-one conversation) identified in Cobb's taxonomy of OSIs [11] may more closely approximate instances in which this analogy is appropriate. Participants in our study did not bring up sub-area OSIs, but we recommend that designers consider whether sub-area OSIs might be appropriate in the context of their app.

Limitations and Future Work

As with other studies that reach participants via Amazon Mechanical Turk, participant bias is a significant limitation of this work – the participants in our study are disproportionately living in the United States, highly-educated, and white. Additionally, in the direct questions we asked about OSI design features (e.g., in the experiment section of the survey), we were not able to address all of the OSI design features that Cobb identified in prior work [11], such as reciprocity of OSI settings, other shapes of OSI icons, and how users' OSIs appear when they are offline. We see promise in future work that includes a more demographically representative survey or that tests users' understanding of additional variants of OSIs.

Additionally, one contribution of the work presented in this paper is that we have identified some specific subpopulations that are especially relevant to consider in follow-up work. For example, the prevalence of many participants who called special attention to the way that family members and romantic partners interpret OSIs points to the importance of understanding how OSIs may play a role in intimate partner violence. Many participants also called attention to how coworkers interpret their OSI. Although workplace environments were one of the original use-cases for OSIs, users may now see their colleagues' OSIs on apps that are not work-related and that are accessed on mobile devices. Future work could explore whether this has shifted the way that OSIs influence a user's experiences at work.

CONCLUSION

In this paper, we conducted an online survey with 200 participants, finding that users often do not understand how OSIs work and have privacy and self-presentation preferences that are not aligned with current OSI designs. OSIs routinely reveal information that users prefer not to share, such as when they are online at odd hours or that they might be avoiding someone. 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. We hope that these findings and the recommendations we make in this work will help app designers make more informed decisions about how OSI design affects user experience.

ACKNOWLEDGEMENTS

We thank Lujo Bauer, Ryan Calo, Dawn Cobb, Ted Mack, Anna Kornfeld Simpson, and John Toman for help with this work in various capacities. We are also thankful for Hannah Almeter and the UW Tech-Policy Lab for their contributions. This work was supported in part by the UW Tech Policy Lab and the Short-Dooley Professorship.

REFERENCES

[1] Daniel Avrahami and Scott E. Hudson. 2006. Responsiveness in Instant Messaging: Predictive Models Supporting Inter-personal Communication. In *CHI*.

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

[3] James "Bo" Begole, John C. Tang, Randall B. Smith, and Nicole Yankelovich. 2002. Work Rhythms: Analyzing Visualizations of Awareness Histories of Distributed Groups. In *CSCW*.

[4] Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor. 2011. Capturing Location-privacy Preferences: Quantifying Accuracy and User-burden Tradeoffs. *Personal Ubiquitous Comput.* (2011).

[5] Michael S. Bernstein, Eytan Bakshy, Moira Burke, and Brian Karrer. 2013. Quantifying the Invisible Audience in Social Networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*.

[6] Igor Bilogrevic, Kévin Huguenin, Berker Agir, Murtuza Jadliwala, and Jean-Pierre Hubaux. 2013. Adaptive Information-sharing for Privacy-aware Mobile Social Networks. In *UbiComp*.

[7] Sara A. Bly, Steve R. Harrison, and Susan Irwin. 1993. Media Spaces: Bringing People Together in a Video, Audio, and Computing Environment. *Commun. ACM* 36, 1 (Jan. 1993).

[8] Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger, and Gernot Bauer. 2011. Falling Asleep with Angry Birds, Facebook and Kindle: A Large Scale Study on Mobile Application Usage. In *MobileHCI*.

[9] Andreas Buchenscheit, Bastian Könings, Andreas Neubert, Florian Schaub, Matthias Schneider, and Frank Kargl. 2014. Privacy Implications of Presence Sharing in Mobile Messaging Applications. In *MUM*.

[10] Matthew Carrasco and Andruid Kerne. 2018. Queer Visibility: Supporting LGBT+ Selective Visibility on Social Media. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*.

[11] Camille Cobb. 2019. *User-to-User Privacy in Social and Communications Applications*. Ph.D. Dissertation. University of Washington.

[12] Camille Cobb and Tadayoshi Kohno. 2017. How Public Is My Private Life?: Privacy in Online Dating. In *WWW*.

[13] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, when, & What People Want to Share. In *CHI*.

[14] Edward S. De Guzman, Margaret Yau, Anthony Gagliano, Austin Park, and Anind K. Dey. 2004. Exploring the Design and Use of Peripheral Displays of Awareness Information. In *CHI EA*.

[15] Trinh Minh Tri Do, Jan Blom, and Daniel Gatica-Perez. 2011. Smartphone Usage in the Wild: A Large-scale Analysis of Applications and Context. In *ICMI*.

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

[17] Erving Goffman. 1949. The presentation of self in everyday life. *Amer. J. Sociology* (1949).

[18] Saul Greenberg. 1996. Peepholes: Low Cost Awareness of One's Community. In *Conference Companion on Human Factors in Computing Systems (CHI '96)*.

[19] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile?: Technology, Risk and Privacy Among Undocumented Immigrants. In *CHI*.

[20] Shion Guha and Jeremy Birnholtz. 2013. Can You See Me Now?: Location, Visibility and the Management of Impressions on Foursquare. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*.

[21] Jeff Hancock, Jeremy Birnholtz, Natalya Bazarova, Jamie Guillory, Josh Perlin, and Barrett Amos. 2009. Butler Lies: Awareness, Deception and Design. In *CHI*.

[22] Stacie Hibino and Audris Mockus. 2002. handiMessenger: Awareness-Enhanced Universal Communication for Mobile Users. In *Proceedings of the 4th International Symposium on Mobile Human-Computer Interaction (Mobile HCI '02)*.

[23] Eric Horvitz, Paul Koch, Carl Myers Kadie, and Andy Jacobs. 2013. Coordinates: Probabilistic Forecasting of Presence and Availability. *CoRR* abs/1301.0573 (2013).

[24] Roberto Hoyle, Srijita Das, Apu Kapadia, Adam J. Lee, and Kami Vaniea. 2017. Was My Message Read?: Privacy and Signaling on Facebook Messenger. In *CHI*.

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

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

[27] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *CHI EA*.

[28] Heather Richter Lipford, Andrew Besmer, and Jason Watson. 2008. Understanding Privacy Settings in Facebook with an Audience View. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08)*.

[29] Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In *IMC*.

[30] M. Madejski, M. Johnson, and S. M. Bellovin. 2012. A study of privacy settings errors in an online social network. In *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*.

[31] Alice Marwick. 2012. The Public Domain: Surveillance in Everyday Life. *Surveillance Society* 9 (06 2012). DOI:http://dx.doi.org/10.24908/ss.v9i4.4342

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

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

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

[35] Sarita Schoenebeck, Nicole B. Ellison, Lindsay Blackwell, Joseph B. Bayer, and Emily B. Falk. 2016. Playful Backstalking and Serious Impression Management: How Young Adults Reflect on Their Past Identities on Facebook. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*.

[36] Katherine Strater and Heather Richter Lipford. 2008. Strategies and Struggles with Privacy in an Online Social Networking Community. In *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1 (BCS-HCI '08)*.

[37] Eran Toch and Inbal Levi. 2013. Locality and Privacy in People-nearby Applications. In *Ubicomp*.

[38] Jessica Vitak, Stacy Blasiola, Eden Litt, and Sameer Patil. 2015. Balancing Audience and Privacy Tensions on Social Network Sites: Strategies of Highly Engaged Users. *International Journal of Communication* 9 (05 2015).

[39] Jessica Vitak, Cliff Lampe, Rebecca Gray, and Nicole B. Ellison. 2012. "Why Won't You Be My Facebook Friend?": Strategies for Managing Context Collapse in the Workplace. In *iConference*.

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