What a Tangled Web We Weave: Lying Backfires in Location-Sharing Social Media

Xinru Page, Bart P. Knijnenburg, Alfred Kobsa
Department of Informatics, Donald Bren School of Information and Computer Sciences
University of California, Irvine, USA
{xpage, kobsa, bart.k}@uci.edu

ABSTRACT
Prior research shows that a root cause of many privacy concerns in location-sharing social media is people’s desire to preserve offline relationship boundaries. Other literature recognizes lying as an everyday phenomenon that preserves such relationship boundaries by facilitating smooth social interactions. Combining these strands of research, one might hypothesize that people with a predisposition to lie would generally have lower privacy concerns since lying is a means to preserve relationship boundaries. We tested this hypothesis using structural equation modeling on data from a survey administered nationwide (N=1532), and found that for location-sharing, people with a high propensity to lie actually have increased boundary preservation concerns as well as increased privacy concerns. We explain these findings using results from semi-structured interviews.

Author Keywords
Privacy; Lying; Boundary Preservation; Location Sharing; Social Media; Structural Equation Modeling; Survey.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms
Human Factors; Design; Measurement; Theory.

INTRODUCTION
Location-sharing services (LSS) are rapidly inundating the technology landscape, in the guise of dedicated mobile applications (e.g. Foursquare) or location-sharing features incorporated into other social media (e.g. Facebook Places) [67]. Although nearly half of all U.S. adults now have a smart phone, only 10% have tried location-sharing services [62]. And while 74% of smartphone owners are willing to use location-based services such as location-based search, only 18% have ever used geo-social services that share location with other people [74]. As the technology is widely available, many researchers blame various privacy concerns for the slow adoption of LSS [67]. In prior work, Page et al. identified the desire for relationship boundary preservation as one key driver of these location-sharing privacy concerns [50]. They demonstrated that privacy concerns increase when users are concerned about location-sharing technology changing the boundaries of their offline relationships. For example, one interviewee explained how his girlfriend didn’t want him to hang out with friends who she thought were a bad influence. Since LSS would reveal his encounters with these friends, he realized that sharing his location with her could cause problems for their relationship. Once they broke up, he was fine sharing his location with her since he was no longer accountable to her in their new relationship.

In analyzing the qualitative portion of the data from Page et al., we further noticed that some people admitted to lying as a routine privacy management tactic. Lying occurred in face-to-face as well as online interactions as a way to maintain relationship boundaries. Lies were often used to hide information or to avoid going out with someone in favor of going out with others.

Some interviewees were confident that they could get away with such lies, even when sharing their location: “I probably don’t have anything to hide [about my location], but even if I do, I can just cover it up…Just make up some story.” On the other hand, more interviewees expressed concern about being caught in their offline lies if their location were known:

[If] I’m calling in sick...to go somewhere like a three day trip, [I’ll say I’m] sick Friday [and] sick Monday to make it more plausible [because] no one gets better over the weekend… I don't think I’d ever want to reveal my location to my coworkers or my boss.

Here, coworkers would question whether this interviewee is really sick if they could see that he is out of town rather than at home. A quarter of the interviewees brought up similar situations in which they had misled someone as to their whereabouts and feared being caught lying. Examples like these led us to wonder whether one’s propensity to lie also plays a role in shaping one’s location-sharing privacy concerns. On the one hand, people may be less privacy concerned if they feel they can count on lying to facilitate interactions. Indeed, much research characterizes lying as a common practice used to facilitate daily social interactions and to maintain relationship boundaries (e.g. [19]). Studies of deception in computer-mediated interactions show that lying also occurs as a boundary management tactic in...
various mediated communications [27]. On the other hand, people with a propensity to lie may be more privacy concerned for fear of being caught at some point. Moreover, the medium of communication affects one’s ability to tell and detect lies (which may explain why the rates of lying vary across media [28]). In LSS, which typically give an unbiased view of one’s location, these fears and concerns of seasoned liars may thus be aggravated.

Not all interviewees who lie may have admitted it during in-person interviews. Thus, to verify whether or not lying propensity affects location-sharing privacy concerns, we administered a nationwide anonymous survey that probes on the propensity to lie alongside boundary preservation and privacy concerns (N=1532). Using structural equation modeling and a latent factor to represent Propensity to Lie, we establish that this factor has a significant effect on a large majority of privacy concerns. Interestingly, these effects are all positive: one’s propensity to lie increases one’s privacy concerns. Upon integrating Propensity to Lie into the boundary preservation model identified in Page et al. [50], this factor continues to have a positive direct effect on privacy concerns. Additionally, we demonstrate that part of this effect is mediated by boundary preservation concerns (BPC) towards the use of location-sharing services. In other words, Propensity to Lie increases concerns about preserving one’s relationship boundaries in location-sharing social media, and this in turn causes one to be more privacy-concerned. These findings indicate that the privacy management tactic of lying tends to backfire in location-sharing social media.

RELATED WORK
Our work falls at the intersection of research on lies and deception, and research on privacy in location-sharing services. We survey related work in these areas.

Lies and Deception
Lying can be characterized as an act that “deliberately seeks to create a false belief” in the other person [27]. Lies may be enacted for self-interests (e.g. enhancing self-image, avoiding embarrassment) or told in the interest of helping another [20]. Some reasons for lying include interational and relational goals, relieving role strain, achieving high-value outcomes or guarding against high-risk outcomes [16]. Studies estimate that one quarter to one third of all interpersonal interactions involve some sort of deception [14, 28]. The vast majority of these lies are what researchers consider minor deceptions such as pretending to agree with someone or making excuses to avoid interacting with someone [27]. In everyday life, many people lie about a diverse range of topics including their feelings, achievements or failures, plans, actions, and location [19]. This is often for impression management reasons (e.g. a concept popularized by Goffman [26] and further developed in subsequent empirical research by various scholars [38, 39]).

Lies can come in many forms including outright deception, equivocation, plausible deniability, and nondisclosure [47]. Many studies in ubiquitous computing encourage systems to support white lies for plausible deniability [31, 40]. Researchers have even addressed this in contexts where technology is always on [5]. Studies of SMS use have identified diverse ways of creating ambiguity such as using temporal, activity-based and location-based excuses [10].

Many scholars focus on how everyday lies are trivial and do not generally cause much distress [19]. Some even emphasize how it is essential to maintaining close relationships [47]: partners may collaborate to maintain lies or use ambiguity rather than full disclosure [20, 22]. However, other research shows how an act of deception and subsequent concealment may instill anxiety. Deceivers may experience apprehension associated with the fear of being caught, or guilt for violating social expectations [14]. Lying to a partner can result in discomfort, less meaningful interactions, and can even cause the liar to trust their partner less [8]. Lying has even been connected to physiological indicators of stress, such as elevated heart rate [15], and lying tendency linked to survival rates for various forms of cancer [58]. These studies suggest that lying, as a coping mechanism, can have negative physiological side effects.

Rather than being pre-planned, most lies unfold as a reaction during the course of an interaction [17]. Nonetheless, psychological research shows that people differ in their tendency to resort to lying in the face of a threat [23]. In other words, although lying is triggered by a threatening situation, the propensity of a person to tell a lie in that situation is a disposition. Studies have also found that people’s predisposition “to use their defensive maneuvers is somewhat independent of the nature of the threatening situation” [15]. This may help explain why people lie just as much offline as online [8, 17, 28], and that the importance and content of lies [28] and the motivations behind lies are similar across media [47].

However, the rates of lying vary across media, and researchers have different explanations for this. Some authors posit a Social Distance theory in which the liar chooses less rich media to put social distance between themselves and the recipient [19]. Others subscribe to Media Richness theory which views lying as equivocal work that benefits from the richest medium so that the liar can personalize and closely monitor the interaction [28]. Hancock et al. criticized these theories for ignoring three aspects: synchronicity, the ability to record the interaction, and whether the communication partners are co-present [28]. They argue that since most lies are unplanned, lying is better carried out in media that are synchronous, hence increasing the opportunities for deception to occur. Moreover, media that can record an interaction allow people to review the content, which deters lying. Lastly, being physically co-present serves as a deterrent too, since one cannot lie about the shared physical environment nor anything observable by both parties.
Based on media richness theory, one would predict that liars do not prefer LSS since it is a limited interaction that does not allow personalization. Furthermore, it supports a limited version of Hancock et al.’s physical co-presence in that both parties can observe the physical location of the person, which deters lying about it. Real-time sharing and ability to record are also popular features of many LSS, which could further deter lying. In all, it seems that for people with a high propensity to lie, LSS is a contentious medium. It inhibits their natural coping mechanism, which impacts their ability to alleviate privacy concerns.

Although lie scales have been developed in prior literature, this was mostly done to detect positive survey response bias, i.e., the (situation-specific) act of lying as a means for social conformity or impression management [23, 55, 59]. We instead focus on the (situation-independent) propensity of people to lie as a way to manage their relationships. There are also scholars who claim that existing scales confound multiple constructs [24, 55]. When applied to new contexts, some scales have even been shown to assign high lie scores to the most honest respondents since items wrongly assume universal truths [44, 56]. Thus, we develop a new Propensity to Lie scale that focuses on lying as a relationship management tactic.

**Location-Sharing**

Location-sharing technologies come in many guises. They range from automatic, continuous, real-time location-sharing (e.g. Google Latitude) to manual check-ins (e.g. Gowalla, Foursquare), to authorized disclosures in response to requests (e.g. HeyWAY), to location tags (e.g. GPS coordinates appended to a Twitter tweet). There are a range of methods to determine the location of a mobile device including GPS, cell towers, wireless access points, and IP address. Until recently, location-sharing technologies have mainly been studied in the lab using experiments and questionnaires. Privacy has often been a primary emphasis in these studies. Researchers posit that the primary determinants of location disclosure are who is requesting one’s location, when, and why [18, 41, 48]. Recent research has also focused on other aspects of who and found that one’s subjective perception of closeness is enough to predict disclosure in a given set of scenarios [73]. Others focused on weighing disclosure benefits versus risks [67].

Some studies conduct field trials of location-sharing prototypes [33]. Real-time disclosures to a limited group of socially connected participants (e.g. co-workers, family, friends) can be useful for being socially connected, coordinating day-to-day activities, and making sure loved ones are okay [6, 13, 57, 70]. Brown et al. point out that in a household setting, location sharing creates a moral component. Family members have to account for their location and justify deviations [11]. To avoid disclosing too much location information, prototypes support nondisclosure, ambiguity, and varying level-of-detail.

Some researchers have studied publically available location sharing services. Humphreys described how Dodgeball, a text-based application, helped people meet up at venues in the city [32]. Page and Kobsa interviewed adopters and non-adopters of Google Latitude and found that several social forces shape people’s attitudes (norms, reciprocity, symbolism) regardless of whether they had adopted the technology [51]. Boesen et al. studied domestic use of Google Latitude as a way of monitoring and making sure children were where they should be [11]. They point out that despite behavioral improvements, this ability to more easily detect lies undermined the perceived trust in their relationships. Our research concentrates on privacy concerns of users and non-users of publically available LSS.

**Privacy**

There are diverse conceptualizations of privacy [64]. Some prominent definitions are Warren and Brandeis’s “Right to be left alone” [71], Westin’s “claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” [72], and Altman’s “interpersonal boundary regulation” [3]. These definitions depict privacy as the ability to regulate physical, informational or social access.

Location-sharing research often focuses on informational privacy and on sharing information with, or withholding it from, the appropriate people [73]. Some researchers have also found impression management concerns [66], worries about being disturbed or disturbing others [33], and apprehension towards potential stalkers [67].

Researchers highlight similar concerns in other social media. Social network users are concerned about who sees what, often because of the various social spheres (e.g. family, work, friends) that intersect on their Facebook page [7]. Users often limit who sees their profile to a defined audience [43, 65]. Likewise, social media users worry about self-presentation and how others’ postings will reflect on them [68], sometimes getting annoyed or being overwhelmed by too much information from others [21]. Studies have also shown concerns for feeling compelled to interact with others online [41].

Nonetheless, throughout the literature there are also counterexamples to these privacy concerns. Location-sharing in families or close friend groups often engenders social connection rather than privacy concern [6]. People disclose enormous amounts of personal information in social networks despite potential embarrassment or threats to their employment, identity, or safety [1, 2, 46]. Individuals leave intimate details open to strangers online [45] without disclosing those details to their closest relationships [29]. Location-sharing services such as SinglesAroundMe.com or Skout are even used to connect with strangers nearby.

Theories of privacy as boundary regulation may shed some insight on these seeming contradictions. For example, Palen and Dourish [53] extend Altman’s theory [3] of offline
privacy to the online world. Like in the real world, online privacy is a regulation of various boundaries: one’s desired level of privacy can be more open or more closed, and one’s current level of privacy may or may not match what is desired. For example, being cut off from interaction could be a privacy violation that results in the person feeling isolated. Along similar lines, sharing more information is not necessarily a privacy problem.

Page et al. [50] validated a model that explains a motivation behind online boundary regulation in location-sharing social media. They identified the desire for boundary preservation of offline relationships as a root cause of diverse location-sharing privacy concerns. In other words, people’s privacy concerns are higher if they are concerned that location-sharing social media would redefine their offline relationships. They found a direct effect of boundary preservation concern on eight privacy concerns that ranged from informational to interactional to physical privacy (see Table 1 for the specific concerns). Furthermore, they found that increased social media use lowered location-sharing boundary preservation concerns and thus had an indirect effect on privacy concerns. This suggests that as people use more social media, they may become better at, and/or less concerned about, preserving their relationship boundaries. In turn, this lowers their privacy concerns. In this paper, we build upon Page et al.’s findings that boundary preservation is a root cause of privacy concerns.

Integrating the Different Fields
Merging the main findings from these fields, a common pattern emerges: People’s privacy concerns are caused by their need to maintain offline relationship boundaries in an online environment. Lying is a commonly used strategy to maintain existing boundaries. However, some evidence suggests that upholding a lie may be much harder in location sharing systems than in other types of social media, and may therefore increase, not decrease, privacy concerns.

We tested the veracity of these claims as part of a larger study, other parts of which have been published elsewhere [50, 51]. The current paper concentrates on how one’s propensity to lie, a determinant not analyzed in previous work, affects privacy and boundary preservation concerns towards location-sharing social media.

STUDY DESIGN
The data for this analysis comes from a two-phase study that comprises a larger effort to understand social media and location-sharing attitudes and adoption. In the first phase, 21 semi-structured interviews were conducted. In the second phase, a nation-wide survey (N=1532) was administered. For the first time, this paper reports on items measuring a Propensity to Lie factor, the qualitative insights that led to its construction, and new analysis that connects lying propensity to boundary preservation and privacy concerns. We thereby build upon findings by Page et al. [50] that relate privacy to boundary preservation concerns.

Phase 1: Interview study
Past research points out that to understand human computer interaction, it is just as important to study non-use of technology as it is to study use [9, 60]. This is particularly relevant for location-sharing technology. Despite widespread availability of smartphones and location-sharing services, adoption of these services has been low [62, 74]. Understanding concerns of non-users could shed light on what is driving people away from these services. Little is known about who is using social media and who is not [12].

We therefore interviewed users of a real-time location-sharing social medium, Google Latitude, as well as non-users. We conducted 1 to 2 hour semi-structured interviews of 7 location-sharing users, 7 who had explicitly chosen not to adopt Latitude, 4 who had abandoned the technology, and 3 who wanted to use it but could not (because the service was not yet available for their phones). This allowed us to study attitudes and privacy concerns that might impede adoption, as well as those arising from usage after adoption. Thus, our findings are applicable to the user populations as well as those who do not use LSS.

The mean age of the subjects was 28 (ages 21 to mid 40’s) and there were 4 females (one of each type of user/non-users). [51] reports more broadly on adoption barriers uncovered by these interviews, while the current paper focuses on propensity to lie (we described essential details here, for complete interview procedures see [51]).

We used open-coding, purposeful sampling, and constant comparison to generate grounded theory [25]. During coding phase, three types of lying emerged (see next section for items). These lies were sometimes the source of privacy concerns and other times the solution to a potential privacy breach. “Non-lying” also emerged, and was either associated with increased concerns (because these interviewees refused to lie to cover up a sticky situation), or lowered privacy concerns (because non-lying interviewees had nothing to hide). This led us to wonder whether one’s propensity to lie impacts one’s privacy concerns and how. Below we report (for the first time) on the development of items reflecting the three types of lying that we encountered in our interviews.

Phase 2: Nation-wide Survey
Based on qualitative insight derived from grounded theory analysis of those interviews, we developed and administered a geographically balanced survey across the U.S. Items used in the current analysis are a subset of the survey questions. In spring of 2011, we posted the survey in 13 Craigslist cities and invited participation from anyone 18 and older who had resided in the U.S. for at least 5 years (as has been done in other privacy studies to control for culture [54]). Past research shows that liars tend to be aware of their behavior and produce fairly accurate self-reports [34]. Also, anonymous online surveys have been found to elicit more honest responses for deviant behavior (such as lying) than methods where a researcher is present [30]. We did not
require location-sharing or other social media use as a pre-condition for participation. This way, our results would be relevant for understanding both user and non-user attitudes.

The first 50 participants each received a $10 Amazon.com gift card and the first 1000 were entered into a raffle for two $100 gift cards. After removing surveys that failed two or more of seven quality checks (e.g. reverse-coded items, unrealistic completion times), we were left with 1532 valid responses. To make the sample more representative of the U.S. population, we normalized responses from each of the U.S. census-defined geographic regions by their respective metropolitan population sizes. 24.0% of the respondents had tried location-sharing services, 79.0% used social media at least weekly, 54.0% owned smart phones, 59.7% had an unlimited data plan, 66.6% were female, the education level was in line with the U.S. Internet population, and the average age was 35.5 years (range 18-73).

The valid responses were randomly split into thirds. In [50], Page et al. used the first sample for theory construction, and the second sample for its validation. For our analysis, we pool these two samples to test our hypotheses. We refer to this as the original sample (N=1021). Additionally, we use the third untouched sample for the validation of our results. We refer to this as the hold-out sample (N=511). Throughout the paper we cross-validate our results between the original and the hold-out samples, and only report on results that are significant in both samples. This ensures the robustness of our results. The reported outcomes are based on the full sample (N=1532).

Privacy Concern Items
The survey included items that probed on privacy concerns. As reported in [50], items were developed to represent eight of the most common online privacy concerns expressed by interviewees (C1-C8). These ranged from informational (e.g. disclosing private information) to social (e.g. impression management) to physical (e.g. physical access) privacy concerns. Another item was created to represent concern for preserving relationship boundaries (BPC) when using location-sharing services. In [50], Page et al. showed that BPC causes C1-C8. Table 1 lists these items (see [50] for a detailed explanation of the construction of each item).

Location-sharing concern items (BPC, C6-C8) were worded in a way that can be answered by everyone, including non-users. Participants responded to these items on 7-point scales whose values are -3 (Disagree Strongly), -2 (Disagree Moderately), -1 (Disagree Slightly), 0 (Neutral), +1 (Agree Slightly), +2 (Agree Moderately) and +3 (Agree Strongly). Since previous research shows that people’s location-sharing attitudes and concerns are intertwined with attitudes towards social media in general [52], items C1-C5 refer to attitudes towards social media that were indicative of location-sharing concerns.

To check whether privacy concerns C1-C8 could be treated as one or more privacy concern factors, we went beyond what was reported in [50], performing exploratory factor analysis (EFA) on the original sample (N=1021). The items did not constitute a well-fitting factor model since the average inter-item correlation was 0.26, whereas 0.30 is a minimal requirement for factorization [35]. Furthermore, the average variance extracted (AVE) was 0.311, below the 0.5 cut-off for factor creation [35]. These results indicate that there is a relationship between the items, but that the correlation is too low for the items to form a robust measurement scale. In fact, all inter-item correlations were low except C7,C8 (r=0.647) and C3,C5 (r=0.516)1 and these pairs lacked face validity to be considered as a construct. Therefore, items C1-C8 are treated as separate, but correlated, indicators.2

<table>
<thead>
<tr>
<th>BPC</th>
<th>I’m worried LSS will change my relationship with others</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>I am bothered that others share so much information with me</td>
</tr>
<tr>
<td>C2</td>
<td>I am concerned that if I share too much information, I would bother others</td>
</tr>
<tr>
<td>C3</td>
<td>I worry that I might share information with more people than I intend to</td>
</tr>
<tr>
<td>C4</td>
<td>I worry about feeling compelled to interact with others online</td>
</tr>
<tr>
<td>C5</td>
<td>I worry that what my friends share will reflect badly on me</td>
</tr>
<tr>
<td>C6</td>
<td>I’m worried about knowing the social etiquette of using LSS (e.g. who to friend, what to share, etc.)</td>
</tr>
<tr>
<td>C7</td>
<td>I’m concerned about being able to control who sees my location</td>
</tr>
<tr>
<td>C8</td>
<td>I’m worried others would join me at an inappropriate time if I share my location</td>
</tr>
</tbody>
</table>

Table 1. Questionnaire items for boundary preservation and privacy concerns. LSS=location-sharing services

Propensity to Lie
The survey included items about one’s propensity to lie (whether lying offline or online), which have not been previously reported. Here we describe the factor construction and validation. Because lying is a sensitive topic, we decided to represent propensity to lie as a latent factor measured by multiple indicators. For content validity, we drew on the types of lying found from the qualitative data. In analyzing the phase 1 interviews, we found that those who spoke of lying often discussed two or more of the following forms of lying: 1) I lie, 2) Everyone lies, and 3)

1 Correlation of < 0.4 is considered low, 0.4 to < 0.7 is medium, and 0.7 or more is high

2 Our modeling tool, Mplus, treats single indicators as single-item latent factors.
Pretending there are technological limitations as a form of plausible deniability (e.g., pretending to have a bad network connection as an excuse for not answering or not being visible in a location-sharing service). Table 2 shows the items developed to represent each form of lying. We describe the development of each item in detail.

<table>
<thead>
<tr>
<th>Everyone Lies</th>
<th>Everyone lies to get out of doing something</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Lie</td>
<td>Sometimes I tell a lie to avoid something (e.g., I tell someone I don’t have time to go out, but then go out with someone else)</td>
</tr>
<tr>
<td>Technology Lie</td>
<td>Sometimes I use technical difficulties as an excuse (e.g., I pretend I had bad cell phone reception)</td>
</tr>
</tbody>
</table>

**Table 2. Questionnaire items for Propensity to Lie factor**

**Everyone Lies**
Several interviewees thought of lying as a typical behavior used by everyone. One interviewee elaborated on how he hid his actions by removing tags that identified him in Facebook pictures: “I don’t know if my friends [remove tags]. I mean, no one wants to get caught in a lie. I’m sure they must do it.” Asserting that others must untag pictures to avoid getting caught in a lie betrays an underlying assumption: Others are lying as well. Because others are lying, they inevitably will run into similar situations. Consequently, we developed an item to reflect the belief that others also lie. This item also had a purpose beyond being an indicator for propensity to lie. We displayed this item before the other lying items in order to frame the behavior of lying as commonplace. Framing is a common technique to increase the likelihood that respondents will be comfortable admitting to what could be perceived as deviant behavior [61].

**I Tell Lies**
Several interviewees mentioned lying as an offline privacy management tactic to avoid going out with someone:

I do tell somebody [I’m] not available for something. I tell them that I’m not feeling too good – I can’t come out. But I’m actually going out with another group of people that they don’t necessarily get along with.

This is an example of the most common lie among our interviewees. Namely, lying to avoid going out with or being around someone. In general, people used lying as an avoidance strategy, whether it be avoiding people in the physical space or avoiding having to converse online. This is in line with other studies that have found that people lie as a way to guard against unwelcome conversations [69] or to extract themselves from an ongoing interaction [27]. This item therefore probes how much one lies as an avoidance strategy. We purposefully framed this and other items in the context of avoidance motives rather than just asking about lying in general. This was in line with motivations described by interviewees and also increased the social acceptability of our questions.

**Blaming Technology**
As a cover up, people often accused faulty technology. An interviewee explained how he could blame technology if location-sharing ever displayed him as being at an unsavory location: “Oh, there’s a library across the street. Latitude must have been a few feet off.” Making excuses by blaming technology may be a more socially acceptable type of lie since it exploits a sense of ambiguity. This is consistent with past research indicating that technology is a common scapegoat to create plausible deniability [4, 5, 10, 31, 40]. Several interviewees were not comfortable lying outright, but content to allege faulty technology. To capture this form of lying, we developed an item focused on blaming technology.

Respondents rated the three lying items (Everyone Lies, I Lie, Blame Technology) on the same 7-point scale used for privacy concern items (see previous section). Using the survey results, we established the reliability and validity of the Propensity to Lie factor. Because the reliability and validity indices are consistent in both the original and the hold-out samples, we report the statistics for the full sample. The factor loadings are significant at the $p < 0.001$ level and had the following values: Everyone Lies $= 0.647$, I Lie $= 0.883$, Technology Lie $= 0.700$. The Cronbach’s alpha of 0.74 indicates a satisfactory level of internal reliability. The Average variance extracted (AVE) of 0.565 indicates acceptable convergent validity.

**Controls**
The survey had several control questions, including location-sharing use, social media use (a composite of how frequently they use various social media including Facebook, Twitter, Instant Messaging, etc.), smartphone ownership, and having data and/or texting plans. Demographics included age, gender, education, geographical location, marital status and parental status.

**ANALYSIS**
For this analysis, we created a structural model that analyzes the effect of Propensity to Lie on privacy concerns. Then we proceed to integrate Propensity to Lie into the full boundary preservation model presented by Page et al. [50] For both analyses, we use weighted least squares estimator (WLSMV) with ordered categorical indicators as our estimation method. This technique does not assume normality of outcome variables. We checked for outliers (+/-3

---

3 A loading $> 0.7$ is considered high, and a loading $> 0.4$ is considered medium. Accepted cutoff values for the reliability indices: Cronbach’s alpha $> 0.7$, AVE $> 0.5$.

4 Mplus uses probit regression to estimate ordered categorical outcomes.
standard deviations) and used bivariate scatterplots to check for homoscedasticity. All data was within normal ranges.

Initially, we modeled LSS users separately from non-users to see if their attitudes and concerns differ. We found no difference and hence combined these data for our analysis. Thus, a single model accounts for both users and non-users.

**Lying Leads to Privacy Concerns**

In [50], Page et al. showed that boundary preservation concern (BPC) is a root cause of eight identified privacy concerns (C1-C8). To test whether participants' propensity to lie could also be seen as a root cause of these eight concerns, we created a structural equation model in which privacy propensity to lie (Lie) causes these concerns. We fit this model on both samples, removed effects that were not significant in either of the two samples, and ran the resulting model on the full sample. This model had a good fit ($\chi^2(12) = 50.151, p < .001; CFI = 0.991; RMSEA = 0.046, 90\% CI: [0.033, 0.059]; WRMSR = 0.558$). Table 3 summarizes the effects in this model.

<table>
<thead>
<tr>
<th>Concern</th>
<th>Effect of Lie → C1-8</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am bothered that others share so much info</td>
<td>0.183***</td>
</tr>
<tr>
<td>I am concerned that if I share too much info</td>
<td>no effect</td>
</tr>
<tr>
<td>I worry that I might share info more with</td>
<td>0.215***</td>
</tr>
<tr>
<td>I worry about feeling compelled to interact</td>
<td>0.235***</td>
</tr>
<tr>
<td>I worry what my friends share will reflect</td>
<td>0.259***</td>
</tr>
<tr>
<td>I’m worried about knowing social etiquette</td>
<td>no effect</td>
</tr>
<tr>
<td>I’m concerned about being able to control</td>
<td>0.116***</td>
</tr>
<tr>
<td>I’m worried others would join me at an</td>
<td>0.161***</td>
</tr>
</tbody>
</table>

Table 3. The standardized effect of Propensity to Lie on the eight different concerns (C1-C8). *** indicates $p < 0.001$

---

5 A significant chi-square means that the model shows some misfit. However, this statistic is known to be very sensitive in large samples such as ours. As an alternative, one may consider other fit indices, which have the following accepted cut-off values: $CFI > 0.96$, $RMSEA < 0.05$ (within [0.00, 0.10]), $WRMSR < 0.95$.

**Lying Integrated with Boundary Preservation Model**

We subsequently integrated Propensity to Lie into the structural model established in [50], in which social media use decreases boundary preservation concern, and in turn boundary preservation concern increases all eight of the other concerns (refer back to Privacy in the Related Works section for a more detailed description). Specifically, we modeled Propensity to Lie as a cause of both boundary preservation concerns (BPC) and the eight individual privacy concerns (C1-C8).

Although it is possible to conceive a model in which boundary preservation concerns cause an increase in the acts of lying, research has shown that the propensity to lie can be considered a stable predisposition [15, 24] rather than a situation-dependent activity. This warrants our choice of the causal direction “Lie → BPC”.

Would the effect of propensity to lie on boundary preservation concerns be positive or negative? First of all, the results of Lie → C1-C8 suggest that propensity to lie will increase concerns. This is in line with research results that lying can cause significant physiological and mental stress or anxiety [14, 15]; this stress could manifest itself as boundary preservation concerns and privacy concerns in social media. On the other hand, lying can facilitate maintaining relationship boundaries [47], which would mean that propensity to lie decreases boundary preservation concerns.

We tested the integrated model on both the original and the hold-out samples and confirmed that it is consistent between the two samples. We also found that age has a consistent negative effect on the propensity to lie, as well as on social media use. We ran the resulting model on the full sample. This model has an acceptable fit ($\chi^2(42) = 175.059, p < .001; CFI = 0.976; RMSEA = 0.046, 90\% CI: [0.039, 0.053]; WRMSR = 0.989$). Moreover, all effects in the model are highly significant (see Figure 1).

The model shows that lying propensity increases not only various online privacy concerns (C1-C8), but also concerns that location sharing will affect one’s ability to preserve relationship boundaries (BPC). This makes boundary preservation concern a partial mediator that amplifies the effect of lying on privacy concerns.

The resulting model also shows that there is a direct effect of age on social media use and propensity to lie. Interestingly, the indirect effects of age on boundary preservation through social media use and propensity to lie are of similar magnitude but in opposite directions and hence end up canceling each other out. The final outcome is that there is no total effect of age on boundary concerns ($p=0.617$). Consequently, age only affects the eight privacy concerns through Propensity to Lie.

As an aside, we did not find any effects of lying on social media use or vice versa.
Discussion
Lying is often depicted as a common privacy management tactic in offline relationships to mitigate concerns and to maintain relationship boundaries. Although the propensity to lie might alleviate boundary preservation concerns in other online technologies [10, 27], our model shows that in location-sharing social media, lying is likely to backfire and to actually increase privacy concerns. These concerns arise directly from Propensity to Lie, but also from liars’ increased concerns about preserving relationship boundaries. Several interviewees recognized the risks in mixing lying with location-sharing social media:

I don’t want to tell someone, “I can’t go out with you – I’m at home,” and then I go out. That’s dangerous. [There have] been situations where I tell someone I’m not going out tonight and then photos will be posted of me going out... One of my friends was just caught. At happy hour, she told one of her friends she wasn’t going to go out. And we went out and that friend happened to show up at the same restaurant.

Location-sharing services change the premise for carrying out these lies by erasing the physical barriers and making location easily accessible.

Some location-sharing services can be used to increase the plausibility of a lie because they allow people to set an incorrect location. However, our qualitative data suggests that this can be problematic as well. Many interviewees would not consider using software to lie, and were disturbed by others who did. One interviewee forsoaks using technology with friends who are not sharing their true location:

So the point about Latitude is to know where your friends are... And so if I see a person toy with an application, I just won’t pay attention to them on it. So it’s like my confidence in how well they use it.... And so my confidence in the way [person’s name] uses this application...was [broken]. So from now I just won’t pay attention to where he is.

Another interviewee explained how he wasn’t interested in Google Latitude because it allows people to set or type an incorrect location:

People can just say they’re wherever they want to say they are... It changes my perception of using Latitude as opposed to showing your accurate location all the time no matter what the users wanted...[It] becomes this unreliable source of information, becomes this messy thing.

Similarly, some interviewees even perceived the practice of blocking others from seeing location to be a deceptive act. A number of these interviewees avoided location-sharing technology and minimized participation in social media in order to keep themselves from falling into situations where lying would be a tempting solution. Several seemed to take an ethical stance against lying. These interviewees serve as a reminder that features to support lying will not appeal to many, and might backfire on the technology and minimized participation in social media.

For those individuals motivated to avoid bad situations (rather than by ethics), several studies conclude that location-sharing technology should support plausible deniability by obscuring or hiding location [4, 5, 33]. For instance, one interviewee who would not tell blatant lies nor use technology to do so, was keeping his relationship a secret from his parents: “I would visit her but wouldn’t tell my parents. I’d say I’m going to Atlanta to visit my friends. I didn't really fly to Atlanta. Well, I DID fly to Atlanta, but...
it was a lay over on the way to another place.” If he had used location-sharing at that earlier point in time, “I would have manually set it to ‘break’.” In other words, he wanted to maintain a partial truth by freezing his location at Atlanta or going offline and using technology as a scapegoat.

However, we question the extent to which this is possible. Obscuring location or ignoring location requests at certain moments or for certain lengths of time may violate relationship boundary expectations. For example, an employee who calls in sick for four days and whose location is unavailable the entire period might raise suspicions. Worse yet, even honest instances of being offline can then be mistaken as deception. Furthermore, as location-sharing services become more accurate and connectivity improves, and as users learn the available features, blaming technology becomes less of an option. Designers will have to better understand offline relationship dynamics in order to understand what constitutes acceptable interactions online.

Our results did not find any relationship between social media use and lying. This suggests that Propensity to Lie does not affect frequency of social media use in general, or vice versa. However, lying propensity does seem to affect concerns towards specific social media. In location-sharing we find that lying propensity increases concerns, but studies suggest that in other technologies it might decrease concerns (e.g. Hancock et al. describe the benefits of butler lies [27]). It may be that this difference is what causes the relatively slow adoption of location sharing services. We are actively investigating whether this is indeed the case.

We also did not find a consistent significant effect of lying on the concern for bothering others with too much information (C2, see Table 3). Conceptually, one can quickly see why this may be so. The Propensity to Lie factor emphasizes lying as an avoidance tactic for self-interested goals. Thus, it is aimed at limiting communication for the benefit of the liar. This in turn does not result in sharing too much information, nor should self-preservation goals necessarily lead to concern for others. So lying should not impact concerns about bothering others.

Lying also did not have a significant effect on the concern for not knowing the social etiquette of LSS (C6). Upon closer inspection, we see that all of the concerns, except C6, are tangible outcomes that can result from lying. Knowing social etiquette (e.g. who to friend, what to share, etc.) has to do with defining what is considered an infraction or problem in the first place, and this may not be affected by one’s lies.

In contrast to prior deception studies that focused on more homogenous samples (e.g. [10, 27]), we found that the propensity to lie significantly decreases with age. This in turn causes older participants to have lower privacy concerns. We see this play out in some of our interviews. One man explained how, as a youth, he would be especially anxious to control what his parents could see but “not so much anymore” because he is not lying to his parents about where he is. Despite common conceptions that teens don’t care about privacy, research has shown that teenagers actually are privacy concerned, especially in social media context [42]. Our findings shed light on one reason younger users could be more concerned: they tend to lie more.

Our model results were consistent with the hypothesis that lying propensity impacts boundary preservation concern. This direction of causality is also in line with existing theory [15]. Yet, because this is a descriptive study, it is conceivable that there is a mutual effect between lying propensity and boundary preservation concerns and thus, boundary preservation concerns could affect lying propensity over time. However, reversing the direction of causality in our model does not yield significant results. Hence, we are unable to claim a mutual effect, and leave the question to future research.

This paper uncovered lying as one privacy management tactic that affects online privacy and boundary preservation concerns. There may be other traditional social practices that are in conflict with modern location-sharing social media. This work is a first step in exploring the interplay of location-sharing social media, our social practices, and our social relationships. Although the focus of our study was on location-sharing technology, the propensity to lie factor was framed as general practice (offline or online) and many of the privacy concern items were about social media in general, not just location-sharing social media. Thus, we suspect that lying may directly increase online privacy concerns in a broader range of social media than just location sharing systems. Future research should investigate lying and boundary preservation concerns in other social media. Longitudinal studies could also shed light on how privacy-preserving social practices instantiate and evolve in new social media.

CONCLUSION

Our findings bring to the forefront Sir Walter Scott’s admonition, “Oh! What a tangled web we weave when first we practice to deceive!” Our results indicate that lying may complicate matters even more in the online social world. This begs the question: Should technology pave the way to more transparent interactions by making it more difficult to lie? Would this force people to tell the truth, or would people avoid the technology? Or on the other extreme, should technology provide fertile grounds for facilitating lies and aim at reducing people’s resulting concerns? In the middle of describing a detailed feature idea making it “convenient” to lie, one interviewee stopped himself and acknowledged this powerful, and perhaps disturbing, influence of technology:

There are applications which force people to lie, force people to do wrong things. And I may want to take my words back. If you're writing it down, just don't write it down because I don't want to be the reason for such a bad feature.
Technology can influence social dynamics by facilitating certain practices and inhibiting others [37]. If one regards lying as undesirable, do designers have an obligation to protect people from their own propensity to lie? The answer to this may depend on one’s ethical viewpoint. Our recommendation is for technology designers and researchers to think about and study the social and moral impact their technology will have and does have once it is deployed. Technological changes can affect social practice whether we design for it or not [49]. If we understand how social practices are evolving around technology, perhaps the social and moral impacts of new technology do not have to go completely unchecked. In the realm of privacy concerns, our paper provides a first step in that direction.

ACKNOWLEDGMENTS
This work was funded by NSF grants IIS-0308277, IIS-0808783 and CNS-0831526, and by Disney Research. We thank Bonnie Nardi and the anonymous CSCW reviewers for their constructive feedback on prior drafts.

REFERENCES


