Viewing the Viewers: Publishers' Desires and Viewers' Privacy Concerns in Social Networks

Roberto Hoyle
Indiana University
Bloomington, IN
rjhoyle@indiana.edu

Srijita Das
Indiana University
Bloomington, IN
sridas@indiana.edu

Apu Kapadia
Indiana University
Bloomington, IN
kapadia@indiana.edu

Adam J. Lee
University of Pittsburgh
Pittsburgh, PA
adamlee@cs.pitt.edu

Kami Vaniea
University of Edinburgh
Edinburgh, Scotland
kvaniea@inf.ed.ac.uk

ABSTRACT

Social networking sites are starting to provide users with services that expose information about their audiences' composition and behavior, such as LinkedIn's 'Who's viewed my profile' feature. Providing information about content viewers to content publishers, however, raises new privacy concerns for viewers themselves, possibly creating a chilling effect on viewer behavior.

We report on a study of 718 respondents using Mechanical Turk across two surveys to study publishers' (N=402) use and expectations of information about their viewers, and viewers' (N=316) privacy behaviors and concerns in the face of such visibility. Our findings indicate that publishers are generally mindful of viewers' privacy; viewers engage in various self-censorship behaviors in the face of visibility; and in some cases (e.g., dating sites) significant gender differences exist about what information respondents felt should be shared with publishers and required of viewers.

Author Keywords

Privacy; Social Networks; Anonymous Access

ACM Classification Keywords

K.4.1 Computers and Society: Public Policy Issues—*Privacy*

INTRODUCTION

Online services are beginning to enable content publishers to learn details about who is viewing and interacting with their content; e.g., LinkedIn provides information about who has viewed one's profile [24] (Figure 1). This visibility raises new and interesting questions about the privacy of the viewers and the degree to which publishers desire this information.[1] Given the visibility of their actions, viewers need to manage the image they present to publishers [9, 37]. This, in turn, may motivate publishers to attempt to strike a balance between information transparency and viewer privacy. A deeper understanding of the extent to which viewers need and expect privacy when online will help balance the privacy and utility needs of both publishers as well as viewers.

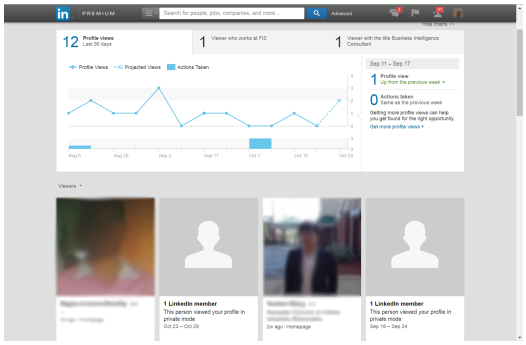


Figure 1: Example of LinkedIn's 'Who's viewed my profile' feature.

The trend toward greater transparency of viewers' actions is not surprising. The lack of information about who is viewing one's content can make it challenging for publishers to adapt their content to their audience and lead to publisher privacy concerns. Without an understanding of their audience, publishers may post information to an unintended set of users [41], potentially leading to lost jobs [8], embarrassment [42], or unfair treatment [30]. These issues have led to a significant amount of research on privacy management in social networks [2, 5, 12]. Recent work explores the concept of providing 'exposure feedback' to publishers, making available data about how and when other people view their information [32].

Providing exposure feedback to content publishers enables them to better manage their privacy [4, 21] but comes at the potential loss of privacy to viewers. When forced to expose their identity, people experience greater pressure to conform

[1] We refer to **publishers** as those people who post their profiles online and **viewers** as those who read the profiles.

CSCW '17, February 25-March 01, 2017, Portland, OR, USA

 ISBN 978-1-4503-4335-0/17/03…$15.00

DOI: `http://dx.doi.org/10.1145/2998181.2998288`

to social norms, leading to less risk taking and lower creativity [37]. Possibly recognizing viewers' potential concerns about their privacy, LinkedIn provides alternatives to disclosing one's identity when viewing other users' profiles: namely, users can instead choose to appear as anonymous or simply display general characteristics about their profile [22]. Users are, however, restricted to the same level of feedback about visits to their own profile.

Despite the benefits to publishers, providing exposure feedback may have a chilling effect on viewer behavior and reduce the overall utility of the social network as a safe space to explore others' profiles and information within certain boundaries. Yet there is little understanding of why and when viewers desire privacy, and how features providing exposure feedback impact viewer behavior. Further, although publishers may find information about their viewers *useful*, they may not necessarily feel that this information should be *required*. We believe that exploring these issues will lead to better design of exposure feedback mechanisms that balance the privacy and information needs of *both the publishers and viewers*, leading to a safer online exchange of information. Specifically, we focus on the following two questions:

R1: *How do publishers currently make use of information about their viewers, and how do viewers modify their behaviors to manage their privacy?* It is not currently understood how and why information about viewers is actually being used by publishers, or whether such exposure feedback has had a chilling effect on viewers. This may shed light on why people desire such privacy and can inform mechanism design for enhancing the privacy of viewers.

R2: *To what degree a) do publishers find various attributes of viewers 'useful'; b) do publishers believe these attributes should be 'required'; and c) are viewers comfortable revealing these attributes?* We seek to understand how people feel about disclosing a range of personal characteristics (e.g., name, age, or gender) in two specific contexts (dating and social networking), and to what degree such information is desirable to publishers. These preferences can inform the design of mechanisms for enhancing the privacy of viewers and also shed light on the tension between the information needs of publishers and the privacy requirements of viewers.

We wanted to consider viewer privacy behaviors in an online interaction situation that supports reciprocal visibility, i.e., where a user as a viewer shares the same information with publishers as the user is able to access about their own viewers. LinkedIn was selected because it is a popular professional networking site and is also used to connect with potential contacts who may not yet be well known to the user. To this end, we surveyed 718 participants using Amazon Mechanical Turk across two surveys: one 'publisher focused' (N=402) and one 'viewer focused' (N=316).

Our findings suggest: (i) users avoid viewing information on LinkedIn because of viewer privacy concerns and do so for several reasons including 'impression management'; (ii) publishers make use of information about their viewers in various ways, such as by researching their viewers but show a concern for the privacy of viewers by indicating that only some types of information should be 'required' in common social networking contexts; (iii) viewers are willing to share personal information with publishers depending on the context (such as dating) and significant gender differences exist. For example, women viewers are less comfortable sharing certain information, but women publishers feel that more information should be required to be shared.

RELATED WORK

Interpersonal Boundary Management

People manage interpersonal boundaries to influence how they are perceived by others in various situations [9]. This can done by controlling what information other people receive, but it can also be about showing respect for others and genuine attempts to highlight ones' most relevant features. This boundary management is continuous and ongoing as people negotiate over time what information is disclosed to others and under which circumstances, such as in the balance between home and work lives. People intermingle them by placement of photos of children on desks while also creating strong barriers by wearing different clothing [29].

One way people negotiate boundaries and impressions is through 'signaling'. Placing a photo of a child on a desk, for example, signals in a quiet way that the person has a child and that this knowledge is public. Signaling allows people to provide information about themselves so that others can, in turn, take that information into account when making decisions or presenting information about themselves. This type of subtle signal is commonly known as a 'weak signal'. Information is provided through a side channel where it can be either followed up on or ignored. Weak signals can be powerful in facilitating human interaction by providing a non-explicit invitation to follow-up on a topic. Bapna et al. studied a dating website that showed people a list of everyone who had viewed their profile (weak signal of interest) and then provided some users with the ability to view profiles without appearing on the list. People who could be anonymous viewed far more profiles but were less likely to find a romantic match due to their inability to leave weak signals [3]. On LinkedIn, the presence of trust and signaling has shown that it is influential in determining who joins a user's network [7].

Exposure Feedback

Completely hiding everything about oneself seems tempting from a privacy perspective. An anonymous person can browse the internet without risk of judgment from others and can therefore be less inhibited and view content that they might not want others to know they have viewed [3, 27]. However, this anonymity means that content authors know little about their audience and may be unable to adapt content appropriately. Authors also have to be more conservative when publishing content to unknown audiences as they have no way of knowing the make-up of the audience or how the audience will react to it [9]. Forcing people to be visible, however, tends to have a chilling effect on their behavior

where they are less willing to explore for fear of giving unintentional signals to others. Thus a balance is needed between publishers' and viewers' demands.

Some researchers have explored 'exposure aware' systems that provide more feedback about how one's information is accessed. For example, Tsai et al. propose an audit-log interface where users can review specific information about who requested their location and when at the end of the day [39]. As an alternative to such detailed information, Schlegel et al. propose an intuitive interface to aggregate and display the frequency of accesses by various classes of viewers [35] providing some degree of privacy to viewers. In general, these systems can provide information about viewers; however, it is not clear how such transparency affects the viewers.

Reciprocity

Other related approaches to address the asymmetry of information exchange between publishers and viewers demand 'reciprocity' from viewers of data, e. g. 'tit for tat' privacy settings in which users requesting someone's location must provide their own location in return [25]. LinkedIn features such a policy for exposure feedback about one's viewers — publishers can see who has viewed their profile only if they are willing to let others know when they have viewed other publishers' profiles [23]. Access controls providing reciprocity have recently begun to gain attention in the access control space, particularly in scenarios where multiple stakeholders with competing interests own content [13, 36].

Data Aggregators

Although the privacy issues of showing information about human viewers to human publishers have been minimally studied in social networks, extensive research has gone into studying the automated tracking of human viewers on webpages [6, 10, 17, 18, 19, 40]. The default setting on most servers is to create logs that track information about visitors such as IP address, browser type, referrer information, and the page visited. Services such as Google Analytics [11] that provide webpage owners with the ability to view information about webpage viewers are very popular and are used by 92% of the top websites [10], suggesting that publishers like to know information about their audiences. Companies also like to know who is viewing their pages; the majority of websites track their viewers and provide personal information to third-party data aggregators [6, 17]. Even prominent US government websites such as HealthCare.gov track viewers and send their personal information, such as pregnancy status to third parties [33].

Users view the collection of information about them by websites as potentially harmful and want them to ask before collecting such data [10]. One of the most visible uses of viewer information has been Online Behavioral Advertising (OBA) where information is used to select advertisements that are individually tailored to a viewer's interests. People have mixed opinions when informed about OBA; some consider it potentially useful while others consider it "creepy" or "scary" [40]. The type of data shared, length of retention, and page context are all factors in viewers' willingness to share information. Viewers are more willing to share general information (e.g., operating system or browser) than more personal information (e.g., address or income). They also prefer to share information with entertainment sites and avoid sharing with banking and dating sites [19].

METHOD

The study consisted of two online surveys focused on understanding respondents' privacy concerns when using social networking systems that provide content publishers with information about content viewers. Although we considered using one survey for both viewers and publishers, there was concern that respondents would be primed by one section when answering the other and that the length would reduce the quality of our responses. To mitigate these concerns, the surveys were split into one asking questions from the viewer's perspective, while the second survey focused on the publisher's perspective. Both surveys were conducted using the Amazon Mechanical Turk (MTurk) service [1]. Although these surveys asked questions about both LinkedIn and Facebook Messenger behaviors, this paper does not report on Facebook Messenger as it is a different kind of service from LinkedIn. We will report on Facebook Messenger in future work.

Survey Instrument

We began with the actions that LinkedIn allows (e.g. connecting, blocking, viewing) as well as actions that are automatically taken for the user (e.g. emailing, suggesting contacts). We brainstormed common reasons for avoiding or disclosing information based on existing impression management research [4, 9, 29, 40]. A pilot was performed to test and refine options, leading to the final survey instrument. It was divided into four sections focusing on: 1) consent form and demographics; 2) questions related to privacy behaviors on LinkedIn as a viewer or publisher; 3) questions related to privacy behaviors on Facebook Messenger as a viewer or publisher; and 4) privacy attitudinal questions related to different, hypothetical contexts as a viewer or publisher. All respondents saw the survey in the same order.

Demographics

The first section included demographic questions about age, gender, nationality, number of people in the household, education, ethnic background, and how long they had been using LinkedIn and Facebook.

Behaviors on LinkedIn

Respondents were asked about their viewer-privacy behaviors and beliefs, including questions about both the available settings and their current settings. The viewer survey asked whether and why viewers had ever avoided viewing profiles or messages because of privacy concerns. The publisher survey asked whether and how publishers had made use of information about viewers. Although several of our questions had free-form text fields, few of our respondents filled them in.

Preferences for different contexts

The final section was about hypothetical sharing of viewers' personal attributes with the publisher (full name, location,

profession, relationship with the viewer or publisher, first name, age group, and gender) in each of five scenarios for the viewer survey (dating, fitness, social networking, photos and location sharing) and in dating and social networking for the publisher survey. As only the data for the social network and dating scenarios on the viewer survey was interesting, we removed the other scenarios from the publisher survey to reduce the burden on our respondents. In this paper we analyze only the common scenarios to both surveys.

Survey instruments

The survey instruments are available as supplementary materials.

Ethical considerations

Participants were compensated $2 for a 20-minute study ($6 an hour). Both surveys were designed to collect no personally identifying information The pilots ensured that the advertised time of 20 minutes was a high estimate. Our organization's ethics board approved the survey and study design.

Recruitment and Validation

Respondents for both surveys were recruited from Mechanical Turk for a "20-min survey on online social networking." To minimize self-selection, privacy was not mentioned in any of the recruitment material.

Responses were screened based on the following criteria: participants were required to be 1) residents of the United States for at least five years to control cultural variations [16]; 2) 18 years of age or older; 3) current users of Facebook and LinkedIn; 4) 'workers' of MTurk with an approval rating of at least 95% to ensure a higher quality of responses. Respondents who 1) correctly answered all attention-check questions; and 2) entered the correct random response code as generated by the survey instrument were included in the data analysis. Respondents who answered one attention-check question wrong were compensated, but their data was excluded.

We published the surveys in multiple batches at various times of the day to obtain a diversity of respondents. The viewer-focused survey was administered from May 6–7, 2015 and the publisher-version from June 29–July 3, 2015.

Respondents

Following our screening criteria, we received 519 and 543 responses respectively for the viewer and publisher surveys. After validation, we were left with a sample of N=316 and N=402 respondents for the viewer- and publisher-focused surveys respectively for a total of 718 respondents.[2] Respondents in both surveys had similar demographics, as detailed in Table 1. Respondents were gender balanced within five percentage points (Male: 52.5% and 47.7% for the viewer and publisher surveys), predominantly White (77.5% and 80%), aged 23–39 (73.7% and 65.1%), and had some college or an undergraduate education (73.7% and 76.3%).

[2]After running the viewer survey, we shortened the survey a bit to make it easier on the Amazon MTurk users by removing some of the scenarios that we decided not to pursue.

	Viewer	Publisher
Gender		
Male	166 (52.5%)	192 (47.7%)
Female	148 (46.8%)	209 (51.9%)
Other	2	1
Age		
18–22	32 (10.1%)	51 (12.6%)
23–39	233 (73.7%)	262 (65.1%)
40–49	33 (10.4%)	58 (14.4%)
50–59	15 (4.7%)	23 (5.7%)
60 and over	3	8
Education		
No high school	0	1
High school	27 (8.5%)	40 (9.9%)
Some college or undergrad degree	233 (73.7%)	307 (76.3%)
Masters	30 (9.5%)	43 (10.6%)
Post-graduate	11 (3.5%)	11 (2.7%)
Ethnicity		
White	245 (77.5%)	322 (80.0%)
Hispanic or Latino	30 (9.5%)	31(7.7%)
African American	25 (7.9%)	35 (8.7%)
Asian	20 (6.3%)	33 (8.2%)
Other	5	1
Total respondents	316	402

Table 1: Demographics of the respondents in the viewer and publisher surveys.

Respondents were asked how frequently they checked profiles on LinkedIn: 62.9% of viewers and 73.1% of publishers reported that they visited one profile a month or more, indicating that they were active users. Another 4.4% of viewers and 2.5% of publishers indicated that they never visited profiles. As the privacy implications of our research questions would affect how frequently one viewed profiles, we retained all responses.

FINDINGS

We present the findings from each of our two research questions in the following sections.

Behaviors of Publishers and Viewers

R1: *How do publishers currently make use of information about their viewers, and how do viewers modify their behaviors to manage their privacy?*

Providing publishers with information about who has viewed their content has the potential to empower them to create content tailored for their audience but may also have a chilling effect on viewer behavior. We report on how the LinkedIn design impacted respondent behavior. In particular, we are interested in both past privacy-preserving actions of respondents and situations where sharing or consuming viewer data was useful.

Awareness

We first look at respondents' awareness of their viewer-privacy options for LinkedIn. This awareness is crucial, as viewers are only likely to take precautionary steps if they are aware of the potential for privacy loss. Respondents were asked under what circumstances a fictional content publisher, Alice, could see the name of someone who viewed her page on LinkedIn.

Publisher and viewer respondents were mostly aware of the viewer-privacy options on LinkedIn with 661 (92.1%) responding that a publisher could 'sometimes' or 'always' see who had viewed their profile. Respondents were also aware that this setting could be controlled with 577 (80.4%) indicating so.

We then asked them to log into their LinkedIn profiles and report their current viewer-privacy settings. A majority of respondents (N=504, 70.3%) had a default setting of full name and headline visible, 96 (13.4%) had their industry and title visible, and 117 (16.3%) appeared as an anonymous viewer. We also asked if they had changed this setting after viewing it. Of the 85 (11.9%) respondents who made changes, 76 (89.4%) of them made a change that increased their anonymity, and three made a change that decreased it.

LinkedIn viewer behaviors

In this section we focus on the 269 (85%) respondents from the viewer survey who were aware that publishers can see who has viewed their profile. We focus on these respondents as they were previously aware that their privacy might be at risk and may have taken action to protect it through self-censorship of their actions.

We asked them whether they had ever deliberately *avoided* viewing someone's profile because of viewer-privacy concerns. Of the 269 respondents, 100 (37.2%) reported that they had avoided viewing someone's profile at least once because of their visibility while 169 (62.5%) reported that they had not. We asked why they had avoided viewing someone's profile, selecting from options shown in Table 2. They were concerned that LinkedIn might send the publisher an automatic email containing the viewer's identity as 50% of respondents reported avoiding viewing someone's profile for this reason. They were also concerned that viewing a profile might signal a personal or professional interest that they didn't want to express. LinkedIn advertises itself as a professional networking site, so the concerns around expressing interest make sense. The responses do suggest that LinkedIn viewers are self-censoring their usage of the system due to privacy concerns.

Viewers on LinkedIn may also find the sharing of viewing information with publishers to be useful. We asked respondents if they had ever deliberately viewed someone's profile on LinkedIn *to cause their name to appear* on the list of 'Who's viewed my profile?' and 43 respondents (16%) answered 'Yes'. We then followed up with a question asking why they had deliberately viewed someone's profile. Responses are summarized in Table 3. Establishing a professional relationship was indicated by 53.5% of the 43 respondents and establishing a personal relationship by 32.6%. The deliberate use of the information-sharing feature shows that respondents are aware of how this type of information is shared and are attempting to use it to their advantage.

Going back to the 47 respondents who believed that publishers were not able to see any information about viewers, we asked if they had ever viewed someone's profile on LinkedIn and been glad that they accessed it anonymously, and 17 of the 47 respondents (36.2%) answered 'Yes'. Again, we asked respondents to select relevant reasons. The main reasons given were relating to relationships, with five (29.4%) not wanting to show a non-existing personal relationship, nine (52.9%) not wanting to show a non-existing professional relationship, and five (29.4%) not wanting to show an existing professional relationship. When asked if they had ever visited someone's profile and wished that the other person had known that they had visited, one participant out of the 47 responded that they had. They said that they wished that LinkedIn had emailed the person about their visit.

Reasons to avoid	Frequency
I did not want LinkedIn to email the other person about my profile visit.	50 (50.0%)
I did not want to reveal a professional interest in the other person (e.g: potential employer, switching jobs).	28 (28.0%)
I did not want to lead the person into believing there is a personal relationship that does not exist.	24 (24.0%)
I did not want to reveal a romantic interest in the other person.	19 (19.0%)
Interacting with this person might reveal something about me I do not want to disclose.	15 (15.0%)
I wanted to pretend I never received a connection request.	14 (14.0%)
I haven't responded to a correspondence from this person and don't want to let them know I have logged into LinkedIn.	14 (14.0%)
I don't want people to know I am checking LinkedIn at that time of day, or day of week.	14 (14.0%)
I did not want to lead the person into believing there is a professional relationship that does not exist.	13 (13.0%)
I did not want this person showing up on my news feed.	11 (11.0%)
To not show someone that they are being ignored	4 (4.0%)
Other	6 (6.0%)
	N =100

Table 2: Reasons why respondents avoided viewing other peoples' profiles.

Reason	Frequency
To establish a professional relationship	23 (53.5%)
To reveal an existing professional interest	16 (37.2%)
To establish a personal relationship	14 (32.6%)
To show that a connection request was received	12 (27.9%)
To reveal an aspect that I want to promote about myself	12 (27.9%)
To have LinkedIn email the other person	10 (23.3%)
To show the other person that I am following them	9 (20.9%)
To show that I logged in at that time	4 (9.3%)
To show that I can log in at that time	1 (2.3%)
To have them show up on my news feed	7 (16.3%)
To reveal an existing romantic interest	3 (7.0%)
	N = 43

Table 3: Top reasons why users deliberately viewed a profile on LinkedIn to cause their name to appear.

LinkedIn publisher behaviors

In the publisher survey, 392 (97.5%) participants indicated that a publisher could 'always' or 'sometimes' see the names of people who visited their page. Only 10 indicated that publishers could 'never' see the names of people viewing their page. The 392 respondents who understood that viewer information was potentially visible to publishers were asked: "In what ways have you made use of the information about 'Who's viewed your profile' page of your LinkedIn account?"

Reasons	Frequency
I visited a viewer's profile	277 (71%)
I researched a viewer online (e.g., web search, looked them up on Facebook, etc.)	138 (35%)
I sent a viewer a connection request	109 (28%)
I directly communicated with a viewer (e.g., email, private LinkedIn message, etc.)	72 (18.4%)
I changed my privacy settings	57 (14.5%)
I asked someone else about this person	53 (13.5%)
I have never made use of such information	47 (12.0%)
I recommended or endorsed a viewer	38 (9.7%)
I blocked or reported a viewer	17 (4.3%)
I shared the profile of a viewer with somebody else	16 (4.1%)
I removed a viewer from my list of connections	14 (3.6%)
I saved the profile of a viewer (e.g., saved to PDF)	7 (1.2%)
	$N = 392$

Table 4: Ways in which participants have made use of the 'Who's viewed your profile' page of LinkedIn

Table 4 shows the list of the possible responses; participants could select as many as they wished.

The majority of participants (N=277, 70.7%) indicated that they had visited a viewer's profile; 138 (35.2%) had researched a viewer online; and 109 (27.9%) had sent a connection request to the viewer. Behaviors reported by approximately 10–20% of the participants included directly communicating with the viewer (18.4%), changing their privacy settings (14.5%), asking someone else about a viewer (13.5%), and recommending or endorsing a viewer (9.7%). Some respondents reported more extreme behaviors such as blocking or reporting the viewer (4.3%) and removing a viewer from their list of connections (3.6%).

Gender and viewer behaviors

Gender was a significant indicator for several viewer-privacy behaviors. Women were statistically more likely than men (47% vs. 29%) to avoid viewing a LinkedIn profile because of the 'Who has viewed my profile?' feature ($\chi^2 = 9.0$, df = 1, p = 0.003).

Viewer-Privacy Needs

Although the findings in the previous subsection focused on actual behaviors in a specific social network (LinkedIn), here we investigate publishers' desires for information and viewers' willingness to provide such information.

R2: *To what degree a) do publishers find various attributes of viewers 'useful'; b) do publishers believe these attributes should be 'required'; and c) are viewers comfortable revealing these attributes?*

In this section of the survey, we asked both the viewer and publisher respondents to provide feedback on accessing or revealing various types of information about viewers in two distinct hypothetical scenarios: dating and social networking. These scenarios represent two common contexts in which a user might desire privacy but might also benefit from sharing information.

For the dating and social networking scenarios, respondents were asked to imagine a website where profile publishers could see some information about the individuals who had viewed their profile. Both groups were provided with a list of viewer information and asked to rate on a 5-point Likert scale how comfortable they would be with sharing the information (viewer survey), if viewers should be required to provide the information (publisher survey), and whether the information would be useful (publisher survey). The results are shown in Figure 2. For brevity we refer to the types of information shared about a person as 'attributes'.

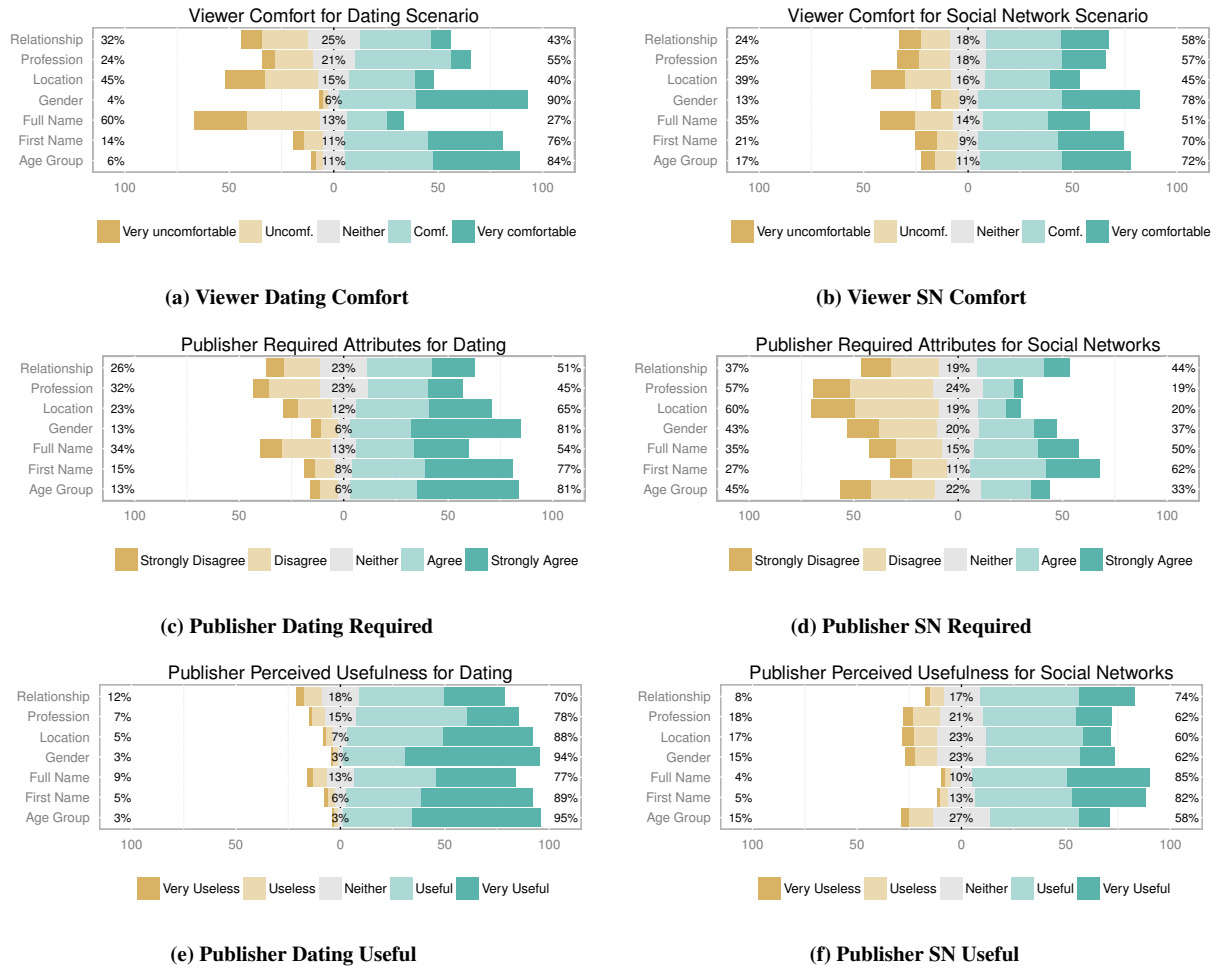
For both surveys, we performed a Friedman test on each scenario to determine if there were any statistically significant differences in responses between the attributes. If so, pairwise Wilcoxon Signed Rank tests were used to test for individual differences. We selected an α of 0.05. A total of 116 pairwise tests were performed, and a Bonferroni correction was applied. All effects are reported at a 0.00043 ($\alpha/116$) level of significance. To minimize the risk of falsely rejecting true findings, we also performed a Benjamini-Hochberg (B-H) correction for comparison.

Dating

Friedman tests revealed that at least one statistically significant difference exists between attributes for both publishers and viewers in the dating scenario ($\chi^2 = 809.6$ for viewers, $\chi^2 = 554.13$ for publishers, d.o.f=6, $p < 0.00001$). Pairwise tests for viewers showed that they were all statistically different from each other except for the difference between Location and Relationship with viewer. For publishers (Table 5), most pairwise tests were statistically significant, except for Full Name with Location and Relationship, Profession with Relationship, and First Name with Gender.

Figure 2 depicts dating site viewers' comfort with sharing attributes (a), publishers' opinion that attributes should be required (c), and how useful publishers' consider the attributes (e). We make the following important observations from Figure 2. Note that the attributes that appear in bold are situations where publishers and viewers had similar opinions and are therefore good candidates for the 'Who's viewed me?' feedback.

1. Publishers find most attributes to be potentially useful, yet they do not feel that all attributes should be required, exhibiting a level of viewer privacy respect.
2. Publishers think that First Name, Age Group, and Gender should be required, and viewers are comfortable revealing these attributes. Viewers' comfort levels for sharing these attributes are significantly different from other attributes, with moderate to large effect sizes indicating that these differences are meaningful. We thus argue that **First Name**, **Age Group**, and **Gender** are *good candidates* for sharing in a 'Who's viewed me?' type listing on a dating site.
3. While publishers tend to agree that Full Name and Location should be required, viewers lean towards not disclosing location, and significantly more so with Full Name. Thus we strongly advise designers of such systems against sharing viewers' Full Names on dating sites even though publishers find it useful. We also advise against sharing location information of viewers and designers should consider privacy controls such as the granularity of a location.



(a) Viewer Dating Comfort

(b) Viewer SN Comfort

(c) Publisher Dating Required

(d) Publisher SN Required

(e) Publisher Dating Useful

(f) Publisher SN Useful

Figure 2: For the *dating* and *social networking (SN)* scenarios how *comfortable* viewers were with sharing attributes (a,b), how much publishers felt the data should be *required* to be shared (c,d), and how *useful* publishers found the data (e,f).

4. Publishers tend to agree that Relationship with Publisher and Profession should be required, and viewers tend to feel comfortable sharing this. Although not significant with the Bonferroni correction, the comfort levels between sharing Location and Relationship with Publisher are significantly different by the B-H correction, albeit with a small effect size. The difference between comfort levels in sharing Location and Profession is significant with a medium effect size. Thus, we advise designers of such systems that it is useful and acceptable to share **Relationship**, and even more acceptable to share **Profession** (the difference is statistically significant with a low effect size).

Social Networks

Friedman tests showed statistically significant differences between attributes for both publishers and viewers in the social networking scenario ($\chi^2 = 347$, $p < 0.00001$ for viewers and $\chi^2 = 449$, $p < 0.00001$ for publishers). Pairwise tests are shown in Table 6.

In particular, we observe the following:

1. Viewers are generally comfortable revealing all attributes but are more comfortable revealing First Name, Age Group, and Gender than Full Name and Location (medium effect size) for which they are more neutral. Attitudes for Relationship with Publisher and Profession lie in between.

2. Publishers indicated a stronger preference that First Name be required and statistically significantly weaker preferences (with medium effect sizes) for Full Name and Relationship with Poster to be required. Viewers were statistically significantly more comfortable with revealing Relationship with Poster than Full Name (with a medium effect size). We thus advise designers of such systems that it is useful and acceptable to share the **First Name** of viewers and only marginally useful and acceptable to share the viewer's **Relationship with Poster**. Other attributes (Gender, Age Group, Location, and Profession), although apparently acceptable from the viewers' perspec-

Categories			T-stat	P-value	Effect
Viewer					
Full Name (2)	<	Location (3)	3989	< 0.0001*†	-0.28
Full Name (2)	<	Profession (4)	2245	< 0.0001*†	-0.55
Full Name (2)	<	Relationship (3)	2913.5	< 0.0001*†	-0.43
Full Name (2)	<	First Name (4)	176.5	< 0.0001*†	-0.72
Full Name (2)	<	Age Group (4)	509.5	< 0.0001*†	-0.73
Full Name (2)	<	Gender (5)	435.5	< 0.0001*†	-0.75
Location (3)	<	Profession (4)	3684	< 0.0001*†	-0.35
Location (3)	<	Relationship (3)	6140.5	0.001†	-0.18
Location (3)	<	First Name (4)	2290	< 0.0001*†	-0.58
Location (3)	<	Age Group (4)	1035	< 0.0001*†	-0.68
Location (3)	<	Gender (5)	401	< 0.0001*†	-0.72
Profession (4)	>	Relationship (3)	7641	< 0.0001*†	-0.23
Profession (4)	<	First Name (4)	2838.5	< 0.0001*†	-0.43
Profession (4)	<	Age Group (4)	1472.5	< 0.0001*†	-0.59
Profession (4)	<	Gender (5)	570	< 0.0001*†	-0.69
Relationship (3)	<	First Name (4)	1479	< 0.0001*†	-0.57
Relationship (3)	<	Age Group (4)	899.5	< 0.0001*†	-0.65
Relationship (3)	<	Gender (5)	415.5	< 0.0001*†	-0.72
First Name (4)	<	Age Group (4)	926.5	< 0.0001*†	-0.27
First Name (4)	<	Gender (5)	233.5	< 0.0001*†	-0.44
Age Group (4)	<	Gender (5)	136.5	< 0.0001*†	-0.33
Publisher					
Full Name (4)	<	Location (4)	4968.5	< 0.0001*†	-0.23
Full Name (4)	>	Profession (3)	8146	0.03†	-0.11
Full Name (4)	=	Relationship (4)	8284	0.749	-0.02
Full Name (4)	<	First Name (4)	1109.5	< 0.0001*†	-0.47
Full Name (4)	<	Age Group (4)	971	< 0.0001*†	-0.52
Full Name (4)	<	Gender (5)	507.5	< 0.0001*†	-0.54
Location (4)	>	Profession (3)	11612	< 0.0001*†	-0.35
Location (4)	>	Relationship (4)	11202	< 0.0001*†	-0.22
Location (4)	<	First Name (4)	2672.5	< 0.0001*†	-0.31
Location (4)	<	Age Group (4)	872	< 0.0001*†	-0.44
Location (4)	<	Gender (5)	966.5	< 0.0001*†	-0.47
Profession (3)	<	Relationship (4)	3830.5	0.006†	-0.14
Profession (3)	<	First Name (4)	1523.5	< 0.0001*†	-0.53
Profession (3)	<	Age Group (4)	651.5	< 0.0001*†	-0.59
Profession (3)	<	Gender (5)	729	< 0.0001*†	-0.6
Relationship (4)	<	First Name (4)	2237.5	< 0.0001*†	-0.47
Relationship (4)	<	Age Group (4)	1208.5	< 0.0001*†	-0.54
Relationship (4)	<	Gender (5)	950	< 0.0001*†	-0.56
First Name (4)	=	Age Group (4)	1177	0.003	-0.15
First Name (4)	<	Gender (5)	1042	< 0.0001*†	-0.24
Age Group (4)	<	Gender (5)	291.5	0.033	-0.11

Table 5: Wilcoxon Signed-Rank test results for Dating, showing differences (median values reported) in a) comfort levels of viewers with disclosing attributes and b) agreement levels of publishers for requiring attributes. Differences significant after the Bonferroni correction are indicated with a '*'; differences significant after the B-H correction are indicated with a '†'. The direction of the difference is indicated by '<', '>', or '='.

Categories			T-stat	P-value	Effect
Viewer					
Full Name (4)	>	Location (3)	4785.5	0.033†	-0.12
Full Name (4)	<	Profession (4)	1446	0*†	-0.22
Full Name (4)	<	Relationship (4)	1363.5	< 0.0001*†	-0.26
Full Name (4)	<	First Name (4)	419.5	< 0.0001*†	-0.45
Full Name (4)	<	Age Group (4)	833.5	< 0.0001*†	-0.47
Full Name (4)	<	Gender (4)	352	< 0.0001*†	-0.54
Location (3)	<	Profession (4)	1119	< 0.0001*†	-0.33
Location (3)	<	Relationship (4)	2329.5	< 0.0001*†	-0.32
Location (3)	<	First Name (4)	1266	< 0.0001*†	-0.45
Location (3)	<	Age Group (4)	450.5	< 0.0001*†	-0.53
Location (3)	<	Gender (4)	197.5	< 0.0001*†	-0.58
Profession (4)	=	Relationship (4)	1675	0.387	-0.05
Profession (4)	<	First Name (4)	1157	< 0.0001*†	-0.28
Profession (4)	<	Age Group (4)	820	< 0.0001*†	-0.37
Profession (4)	<	Gender (4)	269	< 0.0001*†	-0.48
Relationship (4)	<	First Name (4)	618.5	< 0.0001*†	-0.28
Relationship (4)	<	Age Group (4)	841	< 0.0001*†	-0.36
Relationship (4)	<	Gender (4)	283.5	< 0.0001*†	-0.47
First Name (4)	=	Age Group (4)	1014.5	0.017	-0.13
First Name (4)	<	Gender (4)	438	< 0.0001*†	-0.29
Age Group (4)	<	Gender (4)	28.5	< 0.0001*†	-0.25
Publisher					
Full Name (3)	>	Location (2)	18225	< 0.0001*†	-0.48
Full Name (3)	>	Profession (2)	18718	< 0.0001*†	-0.51
Full Name (3)	>	Relationship (3)	9356.5	0.012†	-0.13
Full Name (3)	<	First Name (4)	3394.5	< 0.0001*†	-0.25
Full Name (3)	<	Age Group (3)	11859.5	< 0.0001*†	-0.29
Full Name (3)	<	Gender (3)	9532	< 0.0001*†	-0.23
Location (2)	=	Profession (2)	5065.5	0.457	-0.04
Location (2)	<	Relationship (3)	2414	< 0.0001*†	-0.43
Location (2)	<	First Name (4)	1601	< 0.0001*†	-0.58
Location (2)	<	Age Group (3)	3795	< 0.0001*†	-0.28
Location (2)	<	Gender (3)	3089	< 0.0001*†	-0.34
Profession (2)	<	Relationship (3)	1730	< 0.0001*†	-0.44
Profession (2)	<	First Name (4)	859	< 0.0001*†	-0.61
Profession (2)	<	Age Group (3)	2329.5	< 0.0001*†	-0.3
Profession (2)	<	Gender (3)	2089	< 0.0001*†	-0.36
Relationship (3)	<	First Name (4)	2407	< 0.0001*†	-0.37
Relationship (3)	>	Age Group (3)	9536	< 0.0001*†	-0.21
Relationship (3)	>	Gender (3)	8143.5	0.014†	-0.12
First Name (4)	>	Age Group (3)	15170.5	< 0.0001*†	-0.53
First Name (4)	>	Gender (3)	13247.5	< 0.0001*†	-0.49
Age Group (3)	<	Gender (3)	1093.5	0.008†	-0.13

Table 6: Wilcoxon Signed-Rank test results for Social Networks, showing differences (median values reported) in a) comfort levels of viewers with disclosing attributes and b) agreement levels of publishers for requiring attributes.

tive, were not generally required by publishers and could be suppressed for better viewer privacy.

Gender differences

We compared the preferences for both viewers and publishers when split by gender, summarizing the findings in Table 7. We make the following observations:

1. Female viewers in the dating scenario were statistically significantly less likely than males (with low to medium effect sizes) to be comfortable sharing various attributes (all attributes by the B-H correction).
2. At the same time, female publishers in this scenario were more likely to feel these attributes should be required. These differences are statistically significant (with low to medium effect sizes) for Location using the Bonferroni correction, and for Profession and First Name as well when using the B-H correction.
3. We did not observe any meaningful, or statistically significant, differences in the social networking scenario. We omit details of those tests.

DISCUSSION AND IMPLICATIONS

Our work makes several useful contributions in the context of privacy of viewers in social networks. We found evidence of chilling effects on viewers, mostly due to fear of sending unwanted emails or inadvertent signaling. We found evidence of users viewing profiles to signal interest *deliberately*, mostly to establish a personal or professional relationship, indicating that viewers use the 'Who's viewed me' feature to their advantage as well. For dating and social network sites in general, we make recommendations on which attributes should

Category				T-stat	P-value	Effect
Viewer Dating						
Full Name	M (3)	>	F (2)	16881	< 0.0001*†	-0.33
Location	M (4)	>	F (2)	16298	< 0.0001*†	-0.29
Profession	M (4)	>	F (3)	15064.5	< 0.0001*†	-0.23
Relationship	M (3.5)	>	F (3)	15677	< 0.0001*†	-0.25
First Name	M (4)	>	F (4)	14732.5	0.001†	-0.18
Age Group	M (4)	>	F (4)	14599.5	0.002†	-0.18
Gender	M (5)	>	F (4)	14218.5	0.005†	-0.16
Publisher Dating						
Full Name	M (4)	=	F (4)	18390.5	0.162	-0.07
Location	M (4)	<	F (4)	15966	< 0.0001*†	-0.18
Profession	M (3)	<	F (3)	17260	0.037†	-0.1
Relationship	M (3)	<	F (4)	18427	0.199	-0.06
First Name	M (4)	<	F (4)	16743.5	0.004†	-0.14
Age Group	M (4)	<	F (5)	17821	0.078	-0.09
Gender	M (4)	<	F (5)	17835	0.113	-0.08

Table 7: Wilcoxon Signed-Rank test results for the attributes split by gender.

be shared because both publishers and viewers value them, such as First Name, Age Group, and Gender, and which could be suppressed to enhance viewer privacy as publishers do not seem to require them, such as Full Name and Location. In addition we found differences in behavior and preferences based on gender. Women were more likely than men to avoid viewing a profile and were less likely than men to be comfortable sharing attributes in dating sites, but they were more likely to want them required as publishers.

Our findings have several implications for the design of social networking services, which we discuss next.

Balancing Publisher and Viewer Demands

LinkedIn provides a reasonably high level of transparency compared to other social platforms, but our findings suggest a number of ways that the utility of these mechanisms can be enhanced for both publishers and viewers. Although publishers value feedback regarding the viewers of their content, the degree of feedback desired is by no means set in stone. Further, this feedback can have a chilling effect on viewers, potentially decreasing the traffic to publishers' content. To address this, platforms could provide finer-grained preferences for content providers. This could take the form of altering the *amount* of information collected (e.g., details of individual viewers vs. aggregate view data), as well as *whom* data is collected from (e.g., "Record the *names* of recruiters viewing my profile, and *aggregate counts* of academics who view my profile"). These mechanisms would allow publishers to fine-tune the feedback collected to better meet their needs, while potentially reducing the chilling effects imparted to (classes of) viewers. Of course, reducing chilling effects will require providing viewers with feedback regarding *what* will be collected by visiting a particular profile.

A key finding from our study was that the chilling effects felt by viewers stem, in large part, from a desire to avoid unwanted signaling. This can be addressed by making signaling a first-class action within social platforms. Bapna et al. previously found that weak signals are an important component in facilitating interaction on dating websites [3]. Our work similarly shows that people consider signaling to be an important part of networking sites like LinkedIn for various reasons such as showing professional and personal interest in another person. Unfortunately, privacy settings for viewer privacy are currently coarse-grained and implemented through 'reciprocity' or 'tit-for-tat' policies, where publishers and viewers exchange the same degree of information about each other when viewing each other's profiles.

We envision at least three ways to improve current mechanisms for viewer privacy. First, viewers could be allowed to alter their profile viewing options (i.e., visible vs. private/anonymous mode) on a per-user basis. For instance, an academic pondering a career change might wish to browse corporate profiles anonymously while browsing the profiles of other academics in visible mode. Second, the semantics of anonymous mode could be made more fine-grained. Currently, switching to anonymous mode in LinkedIn completely clears a user's viewer history. One option for a more flexible alternative is that entering anonymous mode means that *future* viewer history will not be recorded for profiles visited in anonymous mode, but *existing* history is preserved. If a profile is later visited in visible mode, viewer history could again be recorded for future views made by the owner of that profile. Third, platforms could provide an alternative to a full view action by enabling viewers to 'peek' at a limited view of a profile or other content *without* signaling to the publisher. For instance, a LinkedIn user might allow anonymous 'peeks' to the (more limited) public version of their profile, but require data collection to see their full profile. These suggestions can improve the exposure feedback mechanisms in the context of location sharing suggested by Tsai et al. [39] (e.g., anonymous peeks at limited amounts of audit log data) and Schlegel et al. [35] (e.g., the eyes interface can reveal names for certain types of information access).

The above design suggestions only scratch the surface of this rich space but illustrate that minor enhancements to the feedback mechanisms deployed by platforms like LinkedIn have the potential to enhance the experience of both publishers and viewers. By leveraging publishers' reported flexibility regarding *what* data they collect and acting on viewers' desires for more *explicit signaling*, platforms could increase the exposure of publishers' content while decreasing the (unwanted) exposure of viewers' private information.

Gender Differences

We found that female respondents were much more likely to avoid viewing a profile than male respondents due to concerns related to what signal this viewing action might appear to send. This finding suggests that controls for weak signaling may be especially useful to women, who may otherwise experience a stronger chilling effect because of the 'Who's viewed me' feature.

We also found gender differences in how male and female respondents were willing to share data in an online dating service. As has been reported previously [14, 20, 38], women are more concerned about revealing their location and other personal details than men, and it follows that they would also be

more concerned, in general, at revealing identifiable information on a dating site. This, again, suggests that emphasizing mechanisms for weak signaling may be especially useful to women, in this case due to preferences against strict reciprocal sharing. Indeed, this finding provides another strong motivation to move away from reciprocal ('tit-for-tat') sharing policies, which may disproportionately disadvantage women by either eroding their privacy or inducing a chilling effect on their participation.

Our findings suggest that a deeper study is needed on gender differences, as women may be adversely impacted by these mechanisms.

Limitations

Our findings are based on self-reported behaviors and attitudes of U.S. participants from the Amazon Mechanical Turk (MTurk) service. Users in general have difficulty accurately recalling their past behaviors [28], and although we endeavored to support recognition of potential behaviors over recall, respondents may have had difficulty accurately recalling past activities. Although MTurk provides a sample of the U.S. population, it has several important biases. Kang et al. found that U.S. Turk workers were "younger and better educated," "put a higher value on anonymity and hiding information," and "had more privacy concerns than the larger U.S. public" [15, 34, 26]. Future studies would need to triangulate our findings using other methods that reach marginalized or technologically removed groups (such as the elderly and people in rural areas and developing countries).

Our survey asks about user's experiences on LinkedIn and may not extend to other social networks. Although some respondents may not have participated in a dating social network, we felt that enough of them would be able to imagine what features they may desire in one.

Some of the differences between MTurk workers and the general population are beneficial for this survey topic. In a general survey it would be challenging to find a sufficiently large sample of people who were aware of LinkedIn's reciprocal sharing of information to be able to study issues such as chilling effects. Surveying MTurkers provides insights into the types of chilling effects experienced by privacy-conscious individuals.

Using MTurk leads to other important concerns related to fatigue and lack of attention. We addressed this through the use of attention checks, which have been shown to increase data reliability [31]. Finally, the complexity of the survey required that it be spread throughout a longer time frame than may have been ideal. We are aware of no events that may have altered our respondent's viewpoints between surveys, and similar questions from each had similar statistical distributions.

CONCLUSIONS

We surveyed two samples of the adult U.S. population to study the privacy concerns and behaviors of people *viewing* (N=316) and *publishing* (N=402) information on social networks. We found that the visibility of viewing behaviors had a chilling effect on participants, who deliberately avoided viewing profiles out of concern for their own privacy. At the same time, we find that publishers are mindful of viewer privacy concerns even though they find information about their viewers useful. Finally, we found gender differences, especially in the context of viewer privacy on dating sites, where women were less comfortable sharing certain kinds of information as viewers while also being more likely as publishers to desire the same information from their viewers.

Our work shows that building a safe, inviting online space requires balancing the privacy and utility needs of both publishers and viewers. Providing feedback about visitors allows publishers to understand their privacy 'exposure', but too much information about viewers can impinge on viewers' privacy and result in a chilling effect. Our findings also shed light on the types of information viewers are comfortable revealing in different circumstances, how gender may play a role in their viewer privacy attitudes, and design implications for making inroads to addressing these issues. We hope that our work spurs further research in analyzing the privacy behaviors and needs of viewers, and the design of privacy settings and mechanisms to balance the privacy needs of both viewers and publishers of information.

ACKNOWLEDGMENTS

This material is based upon work supported in part by the National Science Foundation under grants CNS-1252697 and CNS-1253204.

REFERENCES

1. Amazon Mechanical Turk 2015. Amazon Mechanical Turk. (21 Sep 2015). `https://www.mturk.com/mturk/welcome` (accessed Sep 21, 2015).
2. Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, and Daniel Starin. 2009. Persona: An Online Social Network with User-defined Privacy. In *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication (SIGCOMM '09)*. ACM, New York, NY, USA, 135–146.
3. Ravi Bapna, Jui Ramaprasad, Galit Shmueli, and Akhmed Umyarov. 2013. One-way mirrors and weak-signaling in online dating: A randomized field experiment. In *International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design*, Vol. 3. 2748–2762.
4. 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)*. 21–30.
5. Andrew Besmer and Heather Richter Lipford. 2010. Moving beyond untagging: photo privacy in a tagged world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. 1563–1572.
6. Joseph Bonneau and Soren Preibusch. 2009. The Privacy Jungle: On the Market for Data Protection in

Social Networks. In *Proceedings of the 8th Workshop on the Economics of Information Security*. 121–167.

7. Craig C Claybaugh and William D Haseman. 2013. Understanding professional connections in LinkedInA question of trust. *Journal of Computer Information Systems* 54, 1 (2013), 94–105.
8. Daily Mail 2011. Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook. (07 Feb 2011). **http://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html** (Accessed Sep 21, 2015).
9. Erving Goffman. 1959. *The presentation of self in everyday life*. Garden City, NY Double Day.
10. Joshua Gomez, Travis Pinnick, and Ashkan Soltani. 2009. *KnowPrivacy*. Technical Report. UC Berkeley: School of Information. **https://ashkansoltani.files.wordpress.com/2013/01/knowprivacy_final_report.pdf**
11. Google Analytics. *Google Analytics*. **http://www.google.com/analytics** (accessed Sep 21, 2015).
12. Saikat Guha, Kevin Tang, and Paul Francis. 2008. NOYB: Privacy in online social networks.. In *Workshop on Online Social Networks (WOSN '08)*.
13. Hongxin Hu, Gail-Joon Ahn, Ziming Zhao, and Dejun Yang. 2014. Game theoretic analysis of multiparty access control in online social networks. In *19th ACM Symposium on Access Control Models and Technologies (SACMAT '14)*. 93–102.
14. Harvey Jones and José Hiram Soltren. 2005. Facebook: Threats to privacy. *MIT Technical Report* (2005).
15. Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. In *Symposium On Usable Privacy and Security (SOUPS '14)*. 37–49.
16. Masrur Alam Khan and Rehana Masrur Khan. 2007. Academic Sojourners, Culture Shock and Intercultural Adaptation: A Trend Analysis. *Studies About Languages* 10 (2007), 38–46. Issue 10.
17. Balachander Krishnamurthy, Konstantin Naryshkin, and Craig Wills. 2011. Privacy leakage vs. protection measures: the growing disconnect. In *Proceedings of the Web*, Vol. 2. 1–10.
18. Pedro G. Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. 2012. What Do Online Behavioral Advertising Disclosures Communicate to Users?. In *Workshop on Privacy in the Electronic Society (WPES '12)*.
19. Pedro G. Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers. In *Proceedings of the 9th Symposium On Usable Privacy and Security (SOUPS '13')*.
20. Kevin Lewis, Jason Kaufman, and Nicholas Christakis. 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communications* (2008).
21. Eric Lieberman and Robert C. Miller. 2007. Facemail: showing faces of recipients to prevent misdirected email. In *Proceedings of the 3rd Symposium on Usable privacy and Security (SOUPS '07)*. ACM, 122–131.
22. LinkedIn. *LinkedIn Help Center:"Who's viewed my profile?" - Privacy Settings*. **https://help.linkedin.com/app/answers/detail/a_id/47992** (accessed Sep 21, 2015).
23. LinkedIn. *LinkedIn Help Centre:"Who's viewed my profile?"- Basic and Premium Features*. **https://help.linkedin.com/app/answers/detail/a_id/4508/** (accessed Sep 21, 2015).
24. LinkedIn. *LinkedIn:"Who's viewed your LinkedIn profile?"*. **http://www.alansee.com/whos-viewed-your-linkedin-profile/** (accessed Sep 21, 2015).
25. Hua Liu, Bhaskar Krishnamachari, and Murali Annavaram. 2008. Game Theoretic Approach to Location Sharing with Privacy in a Community-based Mobile Safety Application. In *Proceedings of the 11th International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '08)*. 229–238.
26. Jenny Marder and Mike Fritz. 2015. *The Internet's hidden science factory*. **http://www.pbs.org/newshour/updates/inside-amazons-hidden-science-factory/** (Accessed Sep 24, 2015).
27. Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2008. Shining light in dark places: Understanding the Tor network. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 63–76.
28. Andreas Möller, Matthias Kranz, Barbara Schmid, Luis Roalter, and Stefan Diewald. 2013. Investigating self-reporting behavior in long-term studies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. 2931–2940.
29. Christena E. Nippert-Eng. 1996. *Home and Work*. The University of Chicago Press.
30. Rebecca O'Connor. 2013. Insurance: how a simple query could cost you a premium penalty. (30 Sep 2013). **http://www.theguardian.com/money/2013/sep/30/insurance-query-higher-premiums**(Accessed Sep 21, 2015).

31. Daniel M Oppenheimer, Tom Meyvis, and Nicolas Davidenko. 2009. Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology* 45, 4 (2009), 867–872.

32. Sameer Patil, Roman Schlegel, Apu Kapadia, and Adam J. Lee. 2014. Reflection or action?:how feedback and control affect location sharing decisions.. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*.

33. Cooper Quintin. 2015. HealthCare.gov Sends Personal Data to Dozens of Tracking Websites. (January 2015). **https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-data** (Accessed Sep 21, 2015).

34. Joel Ross, Lilly Irani, M. Six Silberman, Andrew Zaldivar, and Bill Tomlinson. 2010. Who Are the Crowdworkers?: Shifting Demographics in Mechanical Turk. In *CHI '10 Extended Abstracts on Human Factors in Computing Systems (CHI EA '10)*. ACM, New York, NY, USA, 2863–2872.

35. Roman Schlegel, Apu Kapadia, and Adam J. Lee. 2011. Eyeing your Exposure: Quantifying and Controlling Information Sharing for Improved Privacy. In *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS '11)*. 14:1–14:14.

36. Anna Cinzia Squicciarini, Mohamed Shehab, and Joshua Wede. 2010. Privacy policies for shared content in social network sites. *The VLDB Journal* 19, 6 (2010), 777–796.

37. H. Colleen Stuart, Laura Dabbish, Sara Kiesler, Peter Kinnaird, and Ruogu Kang. 2012. Social Transparency in Networked Information Exchange: A Theoretical Framework. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW '12)*. ACM, New York, NY, USA, 451–460.

38. Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2010. Location-sharing technologies: Privacy risks and controls. *ISJLP* (2010).

39. Janice Y. Tsai, Patrick Gage Kelley, Paul Hankes Drielsma, Lorrie Faith Cranor, Jason I. Hong, and Norman M. Sadeh. 2009. Who's viewed you?: The impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. 2003–2012.

40. Blase Ur, Pedro G. Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the 8th Symposium On Usable Privacy and Security (SOUPS '12)*.

41. Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, and Michael K. Reiter. 2012. Out of sight, out of mind: Effects of displaying access-control information near the item it controls. In *PST 2012: Conference on Privacy, Security, and Trust*.

42. Katy Winter. 2014. Daaaaaaad! You're sooooo embarrassing! Almost a third of young people have been 'humiliated' by parents via social media. (16 Apr 2014). **http://www.dailymail.co.uk/femail/article-2605290/Daaaaaaad-Youre-sooooo-embarrassing-Almost-children-humiliated-parents-social-media.html** (Accessed Sep 21, 2015).