Understanding Users' Privacy Attitudes through Subjective and Objective Assessments: An Instagram Case Study

Kyungsik Han, Ajou University
Hyunggu Jung, Kyung Hee University
Jin Yea Jang, Korea Electronics Technology Institute
Dongwon Lee, Pennsylvania State University

Although previous studies have investigated social media users' privacy attitudes, little focus has been placed on understanding the degree of users' concern about different types of private information or the changes in users' privacy attitudes. This article presents novel insights on user attitudes toward 18 privacy items—identified through a review of the literature—and attitudinal changes through a comparative analysis. The authors also discuss the implications of the results that could better support users' privacy management on social media.

0018-9162/18/$33.00 © 2018 IEEE

Over the past few decades, the use of social media has become pervasive and the number of social media users has increased exponentially. A large volume and a wide variety of digital user footprints are generated, from status updates and news sharing to personal photos and videos.[1,2] The very definition of social media necessitates a public profile that articulates a user's personal information, as well as social connections, thus exposing the user's personal information to potential abuse and misuse by service providers, third parties, and even other users. Even though many sites do not ask users for personal information in order to use the service, people are likely to generate and share more categories of private information (henceforth referred to as "privacy items") as they use the service.[1,3–6]

Such a public display of personal information brings forth potential privacy threats. For instance, studies have shown that it is possible to reconstruct social security numbers by using publicly accessible information from Facebook profiles.[7] As privacy issues attract significant attention from the academic research community and mainstream media, social media services allow users to manage their privacy through elaborate privacy settings, thus limiting access to private information. However, research has consistently shown that even though most users are aware of privacy settings, less than half (40 percent) make use of them.[8] Many users do not change the default privacy settings, while approximately 60 to 70 percent of user profiles contain personal or demographic information, such as name, date of birth, city, phone number, interests, and relationship status.

Despite the fact that sharing personal information on social media can lead to severe privacy-related consequences, prior research has revealed that users' self-disclosure seems to be inconsistent with, or uninfluenced by, their privacy concerns. This is known as the privacy paradox.[5,6]

Researchers have adopted many approaches to try to explain the disparity between privacy attitudes and privacy behaviors, indicating that diverse factors (such as demographic differences, usage, technological skills, and social rewards) moderate the relationship between the two.[2,9,10] Researchers have investigated a common or consensus set of privacy items for their research purposes; however, we realized that the categories of privacy items still significantly vary by study, and few privacy items were examined in each study.

We believe an important research action is to comprehensively lay out all privacy items that can be accessed on social media and measure users' attitudes and concerns about each of the privacy items. By taking all potentially sensitive privacy items into account, we can examine and compare user attitudes and behaviors toward privacy items and identify those that are more likely to illustrate privacy discrepancies.

The primary goal of our study is to expand existing privacy research efforts by investigating users' privacy attitudes and behaviors toward 18 privacy items, which were identified through our literature review. We gathered real data and identified user profiles and posts that intentionally, or unintentionally, exposed any of the 18 privacy items. Through a user study, we examined how respondents show changes in privacy attitudes and which privacy items they were most concerned about being exposed. We focused on comparing the respondents' subjective perceptions of the privacy items with their objective selections of the same items. A discrepancy between subjective perceptions and objective selections could imply the case where a user is concerned about a certain privacy item being exposed, but does not illustrate a corresponding action (such as removing or masking the item). Thus, the privacy items that yield discrepancies can be regarded as the privacy paradox.

Overall, our work makes the following contributions.

- We culled 17 privacy items from scattered prior studies (and added one of our own) and applied them to the current study.
- We combined real data that illustrates examples of privacy leakages on Instagram with questionnaire responses.
- We identified a group exhibiting significant changes in privacy attitudes and compared their characteristics with those of other groups exhibiting attitudinal change.
- We highlighted privacy items that could attribute to privacy discrepancies by taking into account respondents' subjective and objective assessments.

RESEARCH MOTIVATION

Our literature review illustrates that the majority of prior studies used surveys as an instrument to measure user behaviors and attitudes toward social media (see Table 1). They relied on a self-evaluation survey method by primarily obtaining respondents' perceptions from a set of questions.[1–6,9]

TABLE 1. Privacy items.

	Acquisti et al.[1]	Blank et al.[3]	Christofides et al.[4]	Taddicken[5]	Tufekci[6]	Boyd and Hargittai[2]	Acquisti and Gross[12]	Young and Quan-Hasse[13]	Kobsa et al.[14]	Quinn[15]	Dwyer et al.[16]	Torres[17]
Birthday	✔	✔	✔	✔		✔						
Education					✔	✔	✔	✔				✔
Email address	✔	✔	✔	✔		✔			✔	✔	✔	✔
Emotions/sentiments				✔	✔							
Family/friend info	✔					✔						✔
Favorites/likes	✔		✔		✔		✔	✔				✔
Home address	✔				✔	✔	✔					
Hometown	✔		✔				✔				✔	
Job				✔	✔	✔						✔
Phone number	✔	✔			✔	✔	✔		✔		✔	
Political views					✔	✔	✔		✔			✔
Postal code		✔										
Profile photo	✔		✔				✔				✔	
Real name	✔	✔		✔							✔	✔
Relationship status			✔			✔			✔			✔
Religion						✔						✔
Sexual orientation					✔						✔	

Although this method is legitimate and offers many insights, it could be better developed. For example, the opinions of users who have not directly experienced privacy infringement (as reflected in conventional polls) could be instantaneous reactions to survey questionnaires and thus lack thoughtfulness.[11]

Some studies used actual data to measure privacy behaviors.[12] However, such studies were conducted in a limited fashion, as few types of information (such as personal information in privacy settings) were used. Moreover, some researchers used manipulated scenarios of privacy leakages,[10] which do not necessarily reflect real examples. We believe that more reliable responses could be collected by presenting users with real cases of privacy exposure occurring on social media.

Our data-driven approach is unique with respect to measuring users' attitudes toward privacy. We asked users to review actual profiles and posts on Instagram and respond to a set of survey questions. Moreover, while a set of arbitrary privacy items was used for measuring users' behaviors and

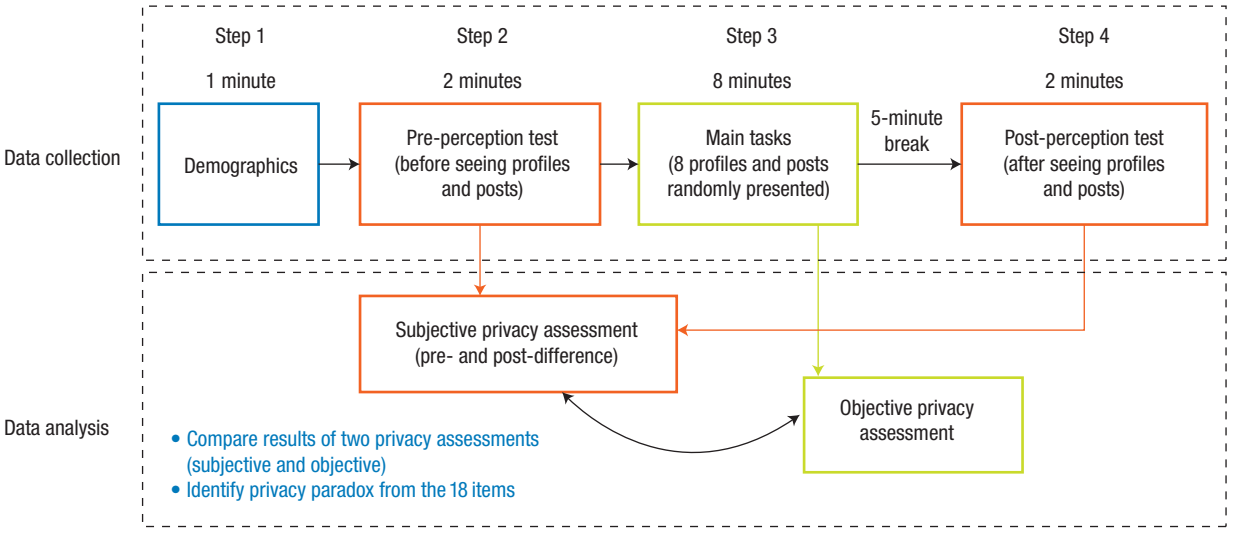

FIGURE 1. Study procedure. We designed a study to measure respondents' subjective and objective selections to observe a privacy discrepancy (a set of the same questions was used in Steps 2 and 4). Subjective privacy assessments (changes in privacy attitudes) were measured through the differences between the pre- and post-tests. Objective privacy assessments were measured in the main tasks. The time for each step indicates the average time taken during each step.

attitudes in prior studies, we compared the impact of each of the 18 privacy items on users' privacy attitudes that could, in turn, positively impact the person's use of social media.

Our literature review allowed us to identify 17 privacy items from prior studies on social media. We added one additional privacy item—other social networking sites (SNSs). Given that using multiple SNSs entails the creation of different social network profiles,[1] users' additional personal information could be identified and obtained from those platforms as well. Table 1 shows the 18 privacy items we identified.

STUDY APPROACH AND DESIGN

We used data collected and distributed by co-author Kyungsik Han et al. (https://goo.gl/LqTYNv), which contains information from 20,000 actual Instagram users who shared their profiles and posts publicly. As for the initial process, we extracted the users who indicated their education level, relationship status, and use of other SNSs through text matching. Consequently, we obtained 477 unique user accounts that met our criteria.

We then counted the number of privacy-related items exposed by manually checking each user's profile and posts. We excluded users who showed less than five privacy items (which is an average of the privacy items revealed from the 477 users), because it allowed us to obtain the 18 privacy items more quickly and efficiently. As a result, we obtained the profiles and posts of 271 users who shared more than five privacy items.

We found that no single user exposed all 18 privacy items. Instead, the number and type of identified privacy items varied across users. Because of this, we decided to group multiple users until we had all 18 privacy items covered in one group. As a result, we had eight users for one complete group that covers all 18 privacy items, creating two user groups. With the two user groups, we asked respondents to view each Instagram user profile in a random order.

User study procedure

Our study was approved by our internal Institutional Review Board. We obtained respondents' consent at the beginning of the survey. Those who consented to the study proceeded with the survey. We used a five-point Likert scale for the questions, where 1 was "not concerned at all" and 5 was "very concerned." We used SurveyMonkey to design and host our survey.

Figure 1 summarizes the study procedure, which was made up of four steps:

- Step 1: We asked respondents to provide their age and gender, as

FIGURE 2. Four examples of a user profile page showing a number of privacy items in the main task. Privacy items were identified from the text and images. We masked user-identifiable information, including faces and usernames. The survey respondents were asked to review different user pages and indicate the degree of their privacy concerns for each of the 18 privacy items for each user page.

well as the average length and frequency of their Instagram use. We also asked them to provide their Instagram username to make sure they were valid users.

- Step 2: We presented respondents with the 18 privacy items and asked them to rate how concerned they would be if each of the private items was revealed on their Instagram profile or posts. This was conducted by asking the following question (through this, we aimed to measure respondents' subjective privacy perceptions):

Question 1: To what extent do you think you would be concerned if the following personal information is revealed on your Instagram page?

- Step 3: Respondents accessed the profiles and posts of real Instagram users. To ensure the privacy and confidentiality of users' private information, we masked their profile images and usernames. We highlighted privacy items with red rectangles and red text (see Figure 2). After accessing the Instagram profiles, the respondents picked the

items that would concern them if they were revealed on their own page. The Instagram pages of the two user groups (with eight users each) were randomly presented to the respondents with the following question (through this, we aimed to measure respondents' objective privacy assessments):

Question 2: Suppose the above profile is yours. Take a close look at the privacy information revealed on the profile. To what extent would you be concerned if any of the above personal information is revealed? Check all that apply.

- Prior to conducting Step 4, we introduced an interval by showing a five-minute video clip to minimize the learning effect.
- Step 4: We asked the same set of survey questions used in Step 2 one more time to observe whether the respondents showed any changes after they completed Step 3. This was conducted to measure the changes that occurred in their privacy attitudes after they were confronted with real cases of privacy leakage.

Respondents

As prior research has demonstrated the reliability and validity of Amazon Mechanical Turks (MTurk),[18] we used this service to collect our responses. The eligibility criteria for respondents were individuals who had at least 95 percent completion rates, who were age 19 or older, who could read and write in English, and who were active Instagram users (had posted 10 or more photos) during the last six months. The survey took approximately 15 minutes to complete.

We collected responses from 293 respondents (157 male and 136 female). The number of respondents who were in their 20s was 167, followed by 99 in their 30s, and 27 who were 40 or older. The average age of the respondents was 29.8 years, with a standard deviation of 8.48. Respondents were active social media users, using social media at least once a day for more than two years. We did not find strong associations between the demographic information and the study results.

RESULTS

Figure 3 illustrates how we defined various user groups for the analysis. For each respondent, we calculated the difference between the pre- and post-test responses to the questions that measure subjective perceptions (see Question 1). We normalized the difference and calculated the mean and standard deviation for each response.

Based on the sum of the mean and standard deviation, we looked at cases with a low pre-test response and a high post-test response (low→high), and cases with a high pre-test response and a low post-test response (high→low). We considered the former as the group of users who exhibited meaningful changes in privacy attitudes because they became more concerned about their privacy after they were shown real examples of privacy leakage. We named this group of 33 respondents the increased concern group (ICG). The other case, consisting of only five respondents, showed a decrease in privacy concerns, even after being exposed to real examples. We named this group the decreased concern group (DCG). Statistically, both ICG and DCG illustrated significant changes between the pre- and post-responses ($p < 0.05$). Because it was uncommon to observe a considerable decrease between the pre-test and post-test responses, we excluded the DCG respondents from further analysis.

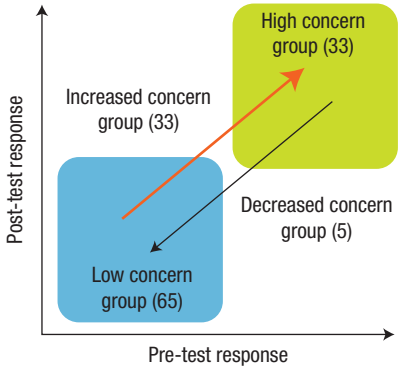

FIGURE 3. Four types of user groups were identified in our study: high concern, increased concern, decreased concern, and low concern.

We defined two more groups from the respondents who belonged to the non-outlier area. One was from both the low pre- and post-test responses (low→low), named the low concern group (LCG). This group consisted of 66 respondents who did not show noticeable changes in privacy attitudes. People in this group were less concerned about their privacy being revealed. Lastly, the 33 respondents who illustrated high pre- and post-test responses (high→high) was named the high concern group (HCG). HCG respondents were highly concerned about their privacy being revealed.

Subjective and objective privacy assessments

We compared the changes regarding the privacy items among the three user groups: ICG, HCG, and LCG. Table 2 summarizes the results, ordered by

TABLE 2. Changes in subjective privacy concerns across three user groups. Privacy items were sorted based on the f-value.*

Privacy item	Increased concern group (ICG)	High concern group (HCG)	Low concern group (LCG)	F(2,128)
Sexual orientation	**1.151**	-0.272	0.123	23.564
Relationship status	**1.212**	-0.181	**0.215**	19.798
Political views	**1.363**	**-0.121**	**0.293**	18.430
Other social networking site (SNS) links	0.878	**0.273**	-0.307	17.160
Hometown	**1.272**	**-0.060**	**0.153**	14.330
Profile photo	0.818	-0.212	**0.200**	14.144
Education	**1.000**	-0.181	-0.061	13.984
Emotions/sentiments	**1.060**	-0.181	0.061	13.925
Family/friend info	**1.030**	-0.272	0.045	12.785
Religion	**1.090**	**-0.121**	0.169	10.271
Postal code	**1.361**	**0.060**	**0.353**	10.188
Birthday	0.818	**-0.151**	-0.123	9.154
Favorites/likes	0.666	-0.212	0.061	9.037
Job	0.698	-0.454	0.000	8.665
Home address	0.909	**-0.030**	-0.015	8.191
Real name	0.606	-0.454	**0.261**	7.842
Phone number	0.909	**-0.090**	**0.153**	6.346
Email	0.969	**0.000**	**0.415**	4.850
Median	0.984	-0.166	0.138	

* Numbers in bold indicate a difference that is greater than the median.

the f-value from the analysis of variance (ANOVA). There were two interesting insights. First, when compared to both HCG and LCG, ICG respondents showed significant increases in privacy concerns across all privacy items ($p < 0.05$). The top three privacy items showing significant differences among the three user groups were sexual orientation, relationship status, and political view. These items illustrated an increase greater than the median (0.984; almost the same as the one-point Likert-scale increase in answers). Secondly, the respondents in both HCG and LCG show small changes in most privacy items, as we assume that people in these groups already had either high or low privacy concerns.

Regarding the objective privacy assessment, we considered the percentage of the selection of each privacy item for the three user groups. All

three groups appeared to make similar selections (see Table 3). Home address, phone number, and family information were the top privacy items selected by all three groups. About 80 percent of ICG respondents chose these three items.

TABLE 3. Objective selections of privacy items of concern during the main task (%), sorted by values from ICG.*

Privacy item	ICG	HCG	LCG
Home address	**88**	**70**	**77**
Phone number	**85**	**73**	**72**
Family/friend info	**79**	**88**	**72**
Email	**67**	58	**68**
Real name	**61**	**64**	**40**
Political views	**52**	55	23
Postal code	**52**	61	**51**
Relationship status	**52**	**64**	20
Emotions/sentiments	48	45	25
Birthday	45	**73**	35
Sexual orientation	45	48	23
Job	42	**73**	32
Other SNS links	39	**79**	29
Religion	39	52	14
Education	36	**76**	31
Favorites/likes	36	48	11
Hometown	36	42	18
Profile photo	30	58	15
Median	51	62	36

* Numbers in bold indicate a difference that is greater than the median.

Item-based privacy discrepancy

With the results of the subjective privacy perceptions and objective privacy selections from the respondents, we answered the following question:

> *Given that people have an ability to control their privacy, what are the privacy items that show discrepancies between subjective perceptions and objective selections?*

From the responses, we obtained early insights into this question by considering together the degree of changes in the subjective perceptions and the objective selections of privacy items. We assumed that each respondent would act consistently during the survey—that is, select the corresponding privacy item if he or she illustrated an increased change in privacy attitude about an item after they saw real examples of privacy leakage. We looked for a case where no selection was made for the privacy item that yielded a significant attitudinal increase. This is how we measured the privacy paradox from the subjective and objective responses.

The results in Figure 4 provide three interesting insights into the discrepancies regarding the privacy items.

First, we found that ICG generally showed greater discrepancies than HCG and LCG. This is because we assume that the respondents in HCG and LCG are likely to have their own beliefs about privacy management (for example, either highly concerned or less concerned).

Second, the red line in each figure indicates the median of the proportion. We see that ICG illustrates nine privacy items (hometown, education, religion, political views, relationship status, profile photo, favorites/likes, emotions/sentiments, and sexual orientation). The red dot next to the bar indicates a discrepancy greater than the median. HCG and LCG show four and five privacy items, respectively. Hometown illustrated the greatest result in both ICG and LCG, implying that many people could easily overlook this privacy item, but might later be concerned about it being revealed.

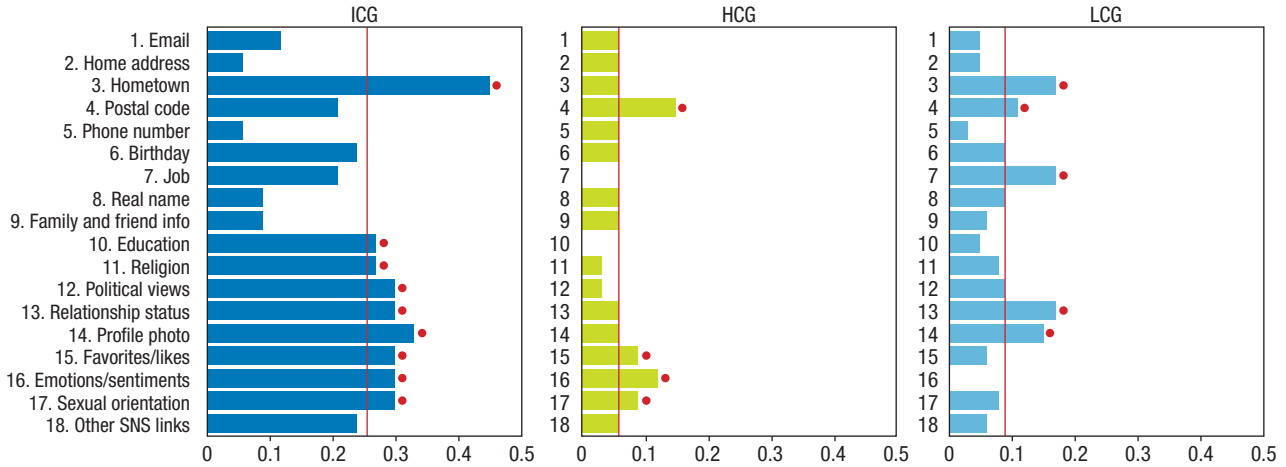

FIGURE 4. Proportion of discrepancies between the subjective attitudinal changes and objective selections across the three user groups. A higher proportion means greater discrepancies. In general, the increased concern group (ICG) illustrated greater discrepancies than the high concern group (HCG) and the low concern group (LCG), as the respondents in HCG and LCG are likely to have their own manner of privacy management. The red line indicates the median of the proportion for each user group. The red dot next to the bar indicates a discrepancy greater than the median.

Finally, we found that hometown, education, religion, political views, emotions/sentiments, and sexual orientation were found in less than 25 percent of the 271 Instagram users in our study but showed higher discrepancies than the average. This implies that the respondents in ICG might still not be aware of the potential of those privacy items being revealed and accessed by others.

We found that various privacy items could easily be revealed on Instagram. The 18 privacy items we identified represent many facets of social media users, but even more categories of personal information that are not covered in our study could exist. We plan to look into additional privacy items through future literature reviews. In addition, as deep-learning techniques for extracting knowledge from images can provide more accurate results, it is expected that more privacy-related information will be identified.

We observed different degrees of attitudinal changes for each privacy item. On the one hand, some of the privacy items such as political view, postal code, and hometown—which are not only the top-ranked privacy items but also showed the greatest changes in ICG—seem to be the ones that many respondents do not realize could have a negative influence. On the other hand, privacy items that are usually accessible on profile pages (such as profile photo and full real name) had relatively smaller attitudinal changes, meaning that fewer respondents changed their minds about these.

Our study shows the importance of considering nine items (hometown, education, religion, political views, relationship status, profile photo, favorites/likes, emotions/sentiments, and sexual orientation) to better preserve users' privacy. Social media sites can and should allow users to take more control over their personal information and posts. A notification feature would be useful, given that many people tend to pay little attention to controlling their privacy. As noted in a previous work, people with lower technical skills could have a tactical disadvantage for managing their privacy in the online space; thus, systematic support would be needed.[19]

Providing examples of actual privacy breaches in the social media space can help mitigate the privacy paradox. This aligns with the notion of "attitudinal inoculation" or "psychological immunization," where misinformation on a certain subject can be "cured" if people are "treated" with a small amount of such misinformation and

informed of how information leakages can pose privacy threats and how they can be countered.[20] It will be worthwhile to examine whether people who exhibit a privacy paradox could be helped if they are confronted with real privacy breach cases.

Although our study presents many interesting insights, we acknowledge a few limitations, which can be addressed in future studies. First, we assessed privacy in social media from respondents who accessed others' Instagram profiles and posts. Although we used real profiles and posts in the study, the study respondents were still in hypothetical scenarios. This might not be optimal in measuring online privacy. Our next step is to run a study using participants' own photos. Second, as indicated previously, because the 18 privacy items are still a small set of all the possible privacy items on social media, we will consider more items in the future. In addition, we will study privacy concerns influenced by the context and effect of the combined privacy items.

Our study offers researcher and practitioner insights on understanding privacy in social media contexts. As we expect that people's use of, engagement with, and dependencies on social media will increase over time, offering users more flexible, user-friendly, and unobtrusive feedback mechanisms is needed for users to better and more efficiently preserve and control their privacy. C

REFERENCES

1. A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science*, vol. 347, no. 6221, 2015, pp. 509-514.
2. D. Boyd and E. Hargittai, "Facebook Privacy Settings: Who Cares?," *First Monday*, vol. 15, no. 8, 2010; http://firstmonday.org/article/view/3086/2589.
3. G. Blank, G. Bolsover, and E. Dubois, "A New Privacy Paradox: Young People and Privacy on Social Network Sites," *Ann. Meeting of the American Sociological Association*, 2014; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479938.
4. E. Christofides, A. Muise, and S. Desmarais, "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" *Cyberpsychology, Behavior, and Social Networking*, vol. 12, no. 3, 2009, pp. 341–345.
5. M. Taddicken, "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure," *J. Computer-Mediated Communication*, vol. 19, no. 2, 2014, pp. 248–273.
6. Z. Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science, Technology & Society*, vol. 28, no. 1, 2008, pp. 20–36.
7. R. Grosa and A. Acquisti, "Information Revelation and Privacy in Online Social Networks," *Proc. 2005 ACM Workshop Privacy in the Electronic Society* (WPES 05), 2005, pp. 71–80.
8. T. Govani and H. Pashley, "Student Awareness of the Privacy Implications When Using Facebook," Privacy Poster Fair at the Carnegie Mellon University School of Library and Information Science, 2015; http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.
9. F. Belanger and R.E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, vol. 35, no. 4, 2011, pp. 1017–1041.
10. B. Reynolds et al., "Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours," *IFIP Conf. Human-Computer Interaction* (INTERACT 11), 2011, pp. 204–215.
11. Y.M. Baek, "Solving the Privacy Paradox: A Counter-Argument Experimental Approach," *Computers in Human Behavior*, vol. 38, 2014, pp. 33–42.
12. A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Int'l Workshop Privacy Enhancing Technologies* (PET 2006), 2006, pp. 36–58.
13. A.L. Young and A. Quan-Haase, "Privacy Protection Strategies on Facebook," *Information, Communication & Society*, vol. 16, no. 4, 2013, pp. 479–500.
14. A. Kobsa, P.B. Knijnenburg, and B. Livshits, "Let's Do It At My Place Instead?: Attitudinal and Behavioral Study of Privacy in Client-Side Personalization," *Proc. SIGCHI Conf. Human Factors in Computing Systems* (CHI 14), 2014, pp. 81–90.
15. K. Quinn, "Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use," *J. Broadcasting & Electronic Media*, vol. 60, no. 1, pp. 61–86.
16. C. Dwyer, S.R. Hiltz, and K. Passerini, "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace," Proc. Americas Conf. Information Systems (AMCIS 07), 2007, https://csis.pace.edu/dwyer/research/DwyerAMCIS2007.pdf.
17. D. O'Brien and A.M. Torres, "Social Networking and Online Privacy:

ABOUT THE AUTHORS

KYUNGSIK HAN is an assistant professor in the Department of Software and Computer Engineering at Ajou University. His research interests include human–computer interaction, social media analysis, and social computing. Han received a PhD in information sciences and technology from Pennsylvania State University. Contact him at kyungsikhan@ajou.ac.kr.

HYUNGGU JUNG is an assistant professor in the Department of Software Convergence at Kyung Hee University. His research interests lie at the intersection of health informatics, human–computer interaction, decision making, data visualization, and social computing. Jung received a PhD in biomedical and health informatics from the University of Washington School of Medicine. Contact him at hgjung@khu.ac.kr.

JIN YEA JANG is a researcher in the Artificial Intelligence Research Center at the Korea Electronics Technology Institute. Her research interests include natural language processing, social computing, and social media analysis. Jang received an MS in information sciences and technology from Pennsylvania State University. Contact her at jinyea.jang@keti.re.kr.

DONGWON LEE is an associate professor in the College of Information Sciences and Technology (iSchool) at Pennsylvania State University. His research interests include data science, particularly data management and mining in diverse forms such as structured records, texts, graphs, social media, and the Web. Lee received a PhD in computer science from UCLA. Contact him at dlee@ist.psu.edu.

Facebook Users' Perceptions," *Irish J. Management*, vol. 31, no. 2, 2012, pp. 63–97.

18. K. Casler, L. Bickel, and E. Hackett, "Separate but Equal? A Comparison of Participants and Data Gathered via Amazon's MTurk, Social Media, and Face-to-Face Behavioral Testing," *Computers in Human Behavior*, vol. 29, no. 6, 2013, pp. 2156–2160.
19. E. Hargittai and A. Marwick, "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy," *Int'l J. Communication*, vol. 10, 2016, pp. 3737–3757.
20. S. van der Linden et al., "Inoculating the Public against Misinformation about Climate Change," *Global Challenges*, vol. 1, no. 2, 2017; doi: 10.1002/gch2.201600008.