Computers in Human Behavior 38 (2014) 296–303

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Understanding privacy knowledge and skill in mobile communication

Yong Jin Park [a,*], S. Mo Jang [b,1]

[a] SLMC, School of Communications, Howard University, USA
[b] School of Journalism and Mass Communications, University of South Carolina, USA

ARTICLE INFO

Article history:
Available online 7 July 2014

Keywords:
Information control
Privacy protection
Mobile surveillance
Smartphone
African Americans

ABSTRACT

This study aims to examine mobile-based privacy literacy among young adults across characteristics of mobile use, basic mobile familiarity, and socio-demographic factors. We investigate privacy knowledge and skill among the African American young adults, adopting a mixed design of quantitative and qualitative inquiries. The results showed that less than half of the interviewed users possessed (1) basic information and locational privacy knowledge, (2) privacy skills, and (3) awareness of risk associated with commercial mobile environments. Interestingly, a high level of mobile familiarity did not translate into knowledge as the frequent daily mobile use was not associated with privacy knowledge and skill. In-depth interviews also indicated that functional confusion and misguided confidence confounded the low mobile knowledge and skills. These findings have implications for consumer policy and hint on the need that the FTC in its broader digital literacy initiative incorporates the information need of young adult users among underserved communities.

1. Introduction

Mobile users face complicated privacy decisions. Revealing personal information early in their adult lives without proper knowledge of privacy issues can bring costly consequences. In fact, young users from various communities find themselves in a demanding information environment, with their mobile devices constantly connected to every aspect of their daily lives (Castells, Fernandez-Ardevol, Qiu, & Sey, 2007). Further, the ubiquitous mobile saturation can hinder abilities to manage digital traces of personal identities effectively.

Our study examines mobile-based information and locational privacy (1) knowledge and (2) skill among young adult mobile users, as well as various related social and technological determinants. To empower the young mobile users, it is critical to investigate the various socio-technological factors that may contribute to or alleviate the acquisition of mobile-based privacy skill, as understanding those determinants can help policymakers design effective interventions targeted at the young populations from different communities. Theoretically, we aim to expand the notion of digital literacy (Park, 2013a) in order to understand personal data protection skill and knowledge in the context of the mobile phone use. Since the mobile access rate has already outpaced Internet penetration, it is essential to recognize how differentiated patterns of mobile privacy literacy contribute to deepening social inequalities.

Recent efforts in privacy studies have been made to examine levels of user knowledge and behavior and a few advanced privacy-surveillance studies made systematic efforts to investigate people's perception and management of public-private boundaries as well as surveillance of mobile-based social network sites (Park, 2013a; Park, Campbell, & Kwak, 2012). Yet, in most mobile studies, surprisingly little has been done to empirically assess personal information skill, while it is critical to understand how users are informed and ready to response to increasing levels of private data collection that mobile devices enable (Campbell & Park, 2008). In this vein, our study addresses three key research questions:

RQ1. How well equipped are young adults in making privacy decisions in mobile use?
RQ2. What are the determinants of mobile-based privacy knowledge and skill?
RQ3. How can policymakers devise effective interventions aimed at the mobile users?

We have a particular interest in the African-American community in which the mobile access is diffused more widely than any

[*] Corresponding author. Address: 13306 Burkitts Road, Fairfax, VA 22033 USA. Tel.: +1 703 657 2181.

E-mail addresses: yongjinp@hotmail.com (Y.J. Park), jangpro@umich.edu (S. Mo Jang).

[1] Address: Carolina Coliseum 600 Assembly Street Columbia, SC 29201.

http://dx.doi.org/10.1016/j.chb.2014.05.041
0747-5632/© 2014 Elsevier Ltd. All rights reserved.

other digital devices (Pew Internet, 2010). This is to understand the mobile uses among the young adults but through the lens of a particular community with vested interests in mobile technologies. Given the broadband penetration among African Americans still lags behind other communities, the mobile devices may carry a symbolic significance as they function as primary sites of cultural production and consumption. In other words, the mobile use can provide alternative venues through which young African Americans might gain online access and actively engage in informational activities (Brown, Campbell, & Ling, 2011).

Analytically, by investigating multifaceted influences of (1) mobile access and use, (2) socio-demographics, and (3) basic mobile familiarity, it is possible to examine whether mobile-based skill variation remains systematically related to certain social factors within a particular community as we focuses on the young adults from a marginalized community. Qualitative in-depth interviews in triangulation enable us to capture the equipment of privacy skill and knowledge in more open-ended and naturalistic settings.

1.1. Policy background

Mobile devices have become ubiquitous and their use is common among young adults. A Pew survey (2010) found that 93% of the young adults aged 18–29 now own a cell phone. Yet such ubiquity contrasts with the regulatory void in establishing meaningful protection of personalized information data. Recent Federal Communication Commission (FCC) policy initiatives failed to address the protection of private data and location related privacy violation in mobile devices. As early as 2002, the FCC refused to create a wireless protection law that requires explicit consent over the use of personal data by third parties (FCC order, 2002). Although the Federal Trade Commission (FTC, 2010; 2011) recently weighed different proposals concerning location-tracking, its continued stance on non-intervention remains de facto in void of effective mobile-based privacy protection.

It is in fact widespread that marketers not only collect the personal data, such as locational whereabouts or/and clickstream activities, from mobile platforms, but also appropriate those data to feed into various products and advertising in such mobile app services as Google map or Foursquare. One report suggests that while Internet access in mobile platforms is expected to overtake fixed access by 2014, as much as 29% of the mobile users are willing to release data for discount coupons or similar reward options (Bosomworth, 2013). Although such benefits from individually-tailored marketing are perceivable, those who do not understand and cannot effectively manage mobile-related information surveillance remain potentially vulnerable to egregious violations of privacy.

In 1998, U.S. Congress established the Children Online Privacy Protection Act (COPPA) to limit the data collection of online users under the age of 13. The age-based provision under the COPPA, however, precludes adequate control by adult users to curb data abuses. Further, the COPPA that mandates verifiable parental consent in online transactions does not apply to the third party access to mobile-apps that are essential to personalized digital lives. Despite some implication of the COPPA for mobile apps, current legal protection of personal identities and location related application is limited as the details of possible legislations remain unclear (Cottrill, 2011; Franken, 2011). In this regard, the highly publicized recent update of the COPPA clarified that geo-location information, photographs, and videos cannot be collected without parental notice and consent (FTC, 2011). Yet no clear oversight mechanism by the FTC effectively means its continuous reliance on self-regulatory ‘notice and choice’ provision by third party mobile apps providers.

2. Related studies

2.1. Importance of mobile literacy

The rise of interactive mobile technologies in particular is likely to encourage public sharing of personal data and there is strong evidence for Twitter users revealing locational whereabouts in mundane everyday practices (Humphreys, Gill, Krishnamurthy, & Newbury, 2010). In fact, highly wired young users are not necessarily sophisticated in their Internet uses and skills. For example, there are findings that indicate few college students were engaged in creative online activities as this was manifest only among those with higher parental education level (Hargittai & Hinnant, 2008). Supporting this concern, a series of recent U.S. national sample studies (Park, 2013a) found the lack of knowledge about basic marketing surveillance practices among most consumers. Other studies also reported inadequate levels of privacy awareness among college students in their uses of social network site such as the Facebook (Acquisti & Gross, 2006; Fogel & Nehmad, 2008). Collectively, these suggest that there exist strong reasons for social and policy concerns about the young population effectively responding to digitalization of personalized data in mobile-based platforms.

To understand the levels of privacy knowledge and skill among young mobile users, we put forth a new measure of digital literacy that focuses on mobile privacy-related skills and knowledge. Here the notion of mobile privacy literacy describes individual knowledge and skill regarding privacy-related functions in the mobile phone. In explicating the notion, we turn to the notion of “the second-level digital divide” (Hargittai, 2002; Hargittai & Hinnant, 2008). That is, there exist the differences in people’s knowledge and skills of new technologies beyond the binary distinction of the ‘haves’ and the ‘have-nots’ (Park, 2013a). Put it differently, there are many levels of differences in terms of access, the first level, as well as skill and knowledge, the second level. While this understanding is applicable to any new media technologies, we posit that the level of mobile privacy literacy is an essential component of the effective digital participation in mobile phone use as some research suggests that different levels of expertise can promote or inhibit users in specific domains, such as personalized data use and control.

In fact, strong empirical findings in various domains of Internet uses suggest that users remain different at their skill and knowledge levels and particular segments of population are consistently left out from benefits of new technology because there are those who could not fully utilize the technology (DiMaggio, Hargittai, Neuman, & Robinson, 2001; Park, 2013a; Park, 2013b). In this context, it is important to delineate nuanced measures of people’s protective ability in order to understand how the benefits or risks from new technology, such as the mobile phone, become manifest in particular social segments. Nevertheless, there has been the conspicuous absence of empirical endeavors that systemically examine mobile-related knowledge and skill, and an underserved community in specific domains of privacy and information evaluation has never been investigated.

Replicated in much of the earlier mobile studies is the question of cell phone access rate. For instance, the binary mobile-ownership variable was the central locus of inquiry as age, race, and gender (Charski, 2004) disparities persisted at the levels of adoption. However, this approach may suggest that gaining access to the mobile obliterates any potential skill underdevelopment that may result from lack of access to the new medium. That is, people’s capacities to best utilize and understand new technology are assumed to be in par with the increased level of access. This exacerbates a notion that the explosion of mobile phone ownership is the same as social preparedness in use, although no systematic attention has been paid to marginalized user groups. In other words, societal readiness to utilize and understand the new medium remains underexplored beyond the concern of penetration and issues of skill readiness in diverse dimensions of information privacy rarely came forward in understanding specific user groups.

While it is important to note that mobile privacy remains understudied with regard to the youth in the context of marginalized communities, several studies found that non-white users tended to fall behind in privacy control behavior (Park et al., 2012) and knowledge (Park, 2013a). Other empirical studies also expressed consistent concern about children and young people's privacy in terms of parental supervision (Livingstone, 2007), contextual nuances of daily activities (Grant, 2006), and peer connection and socialization (Ito & et al., 2008).

In this vein, we posit that the African American young adults are particularly significant to consider. On the one hand, the African American young adults – with the highest rate of access to personal mobile devices (Pew Internet, 2011), grow up in the mobile-saturated life environments. On the other hand, there are other societal concerns that are specific to African American community, of which the poverty rate has recently exacerbated, surpassing those of other communities (US census, 2011). Furthermore, the limited life experiences of young adults in the process of cognitive and emotional development may put them at a greater risk of under-developing skill sets. As a consequence, certain segments of African American community, especially those with low social-economic status, income and education levels, may not have due resources to translate high levels of mobile experiences into quality-digital engagements in dealing with personal information.

In summary, we are concerned that while all the population segments may have become increasingly connected through the mobile phone, younger users may not be fully ready. To this end, African American young adults serve as a critical lens through which to raise social and policy concerns with regards to (1) the levels of mobile-based privacy skill and knowledge and (2) the extent of socio-demographic factors in predicting their readiness. Granted that our study is particularly interested in the unique problem concerning underserved communities, the value of studying African American young adults lies in the much needed empirical evidence regarding digital readiness among those from one of the most mobile-ready communities.

2.2. Contribution of this study

Hence, the present study advances the prior literature in three important ways. First, our study evaluates the levels of information privacy knowledge and skills among the mobile users, by employing a dataset that focuses on the young adults from a marginalized community. Second, we use multivariate analysis to examine how levels of mobile-based privacy knowledge and skill may differ across socio-demographic factors, characteristics of mobile use and access, and mobile familiarity within the community. Third, the observations that involve in-situ interviews and conversations will identify the key dimensions of knowledge and skill that may not stand out in quantitative assessment. The users of underprivileged communities in their digital skill development and readiness regarding mobile privacy have not been studied yet, despite ubiquitous mobile access. Overall, this study contributes to fill this missing gap in light of devising concrete mobile-based information privacy policy measures.

3. Methods

3.1. Sampling and data collection

We conducted a series of in-depth interviews, and survey analysis. For the purpose of the present analyses, we constructed a composite dataset after the response validity check in the first wave of data collection, adding a new set of data from the second wave in a series of pilot studies. The analyses were based on 60 individual observation sessions. Each session lasted about one hour, including a survey administration and an observation-interview. The study population was recruited, using non-probability purposive and snowballing sampling procedures. For being purposive of seeking young African American adult users, primary recruitment was made from a historically-black college and university (HBCU) campus in a major metropolitan area in the U.S. Those at initial contacts expanded a participant pool by inviting possible participants, using snowballing technique. The participants (18-24) were first invited to a computer lab and took a survey questionnaire, followed by in-depth observation and interview. Snowballing sampling has advantages of recruiting members of underprivileged communities (Burrell, 2010). In addition, because young users often rely on a network of knowledgeable associates or peer, this technique provided us with an effective reference point to understand a target group.

Like any studies that utilize a mixed design of quantitative and in depth observations, the procedure used in this study has limitations. First, the study was confined to a small group of users from one ethnic group in a close social circuit; thus, results may not be overgeneralized to other times and groups dissimilar to this. Participants might also have given socially desirable answers especially with regards to knowledge-related questions. Still, the rich qualitative data offset the potential generalization problems of findings from a small data set. Observations also served to validate participants' responses. To this end, it seems reasonable to look at all possible nuances, including those variables failing to stand out in statistical tests. Further, it has been shown that the small sample size is advantageous in identifying 'natural ways' of a particular population engaging in information behavior (e.g., Tombros, Ruthven, & Jose, 2005).

Table 1 shows the main characteristics of the participants in this study. The levels of education, household income, and gender of the participants reasonably approximated those of the African American population in the U.S. First, our sample was 53.3 percent female. In terms of parental education, the median education level in both this data set and American Community Survey was some college. In our sample, only 26 percent had a father with a B.A. degree or above. The medium income level was higher than that of African American national households. Still, it was reasonably

Table 1
Descriptive characteristics of the participants.

	Study sample 2011–2012	
	Mean	*SD*
Socio-demographic status		
Parental education	3.36	1.13
Age	20.23	2.07
HH income	4.19	1.53
Gender (high: female)	53.3%	
Mobile access		
Hours of daily mobile use	9.54	5.53
Frequency of mobile Internet access	5.22	1.19
Mobile familiarity		
Basic mobile familiarity	20.67	3.38

Note: Both parental education and income were measured in six categories.

close to the African American population as about 40 percent in our sample was below $50,000, while the medium income level among African American households was $33,465 in 2011 and $35,575 in 2008 (US census, 2011).

3.2. Quantitative analysis

3.2.1. Mobile privacy knowledge

Knowledge was operationalized as user awareness in the two dimensions of institutional practices: (1) information and (2) location related mobile personal data. For both dimensions, the participants were asked seven *true-false* questions that rated their understandings of mobile-based surveillance practices. Items were adopted from prior studies (Park, 2013a; Park, 2013b; Pew Research, 2010; Turow, Feldman, & Meltzer, 2005) and were later coded 1 for correct answers with 0 assigned to all other responses (see Table 2 for distribution of individual items) (KR 20=.57).

3.2.2. Mobile privacy skill

Mobile-based privacy skill was measured as use behavior in the two dimensions: (1) information and (2) location related mobile personal data. Respondents were asked to report the extent to which they were involved in each of the information behaviors on a six-point scale (1 = *not at all*, 6 = *all the time*). A total of seven individual items were modified from prior studies (Acquisti & Gross, 2006; Litt & Hargittai, 2014; Marx, 2003; Park, 2013a; Pew Research, 2010) to measure individual skill in responding to mobile-based information-location data use (α = .72).

3.2.3. Predictors

Three types of predictors were used to assess systematic distribution of skill and knowledge. First, demographic characteristics of gender and age were used, along with socioeconomic indicators of household income and parental education. The second type included characteristics of mobile use such as the frequency of mobile Internet access (1 = *never*, 6 = *very often*) and the hour of daily mobile use in order to measure effects of particulars associated with young adult users' mobile experience (Skoric, Ying, & Ng, 2009, for media exposure and Internet use variables). It has been suggested in empirical findings (Park, 2013b) that digital skill inequalities may derive from difference in cognitive technological understanding. To examine this in mobile contexts, the final predictor includes a composite index measure of basic familiarity with mobile-related terms rated with six items (GPS, 3G, roaming, geotagging, WAP, and bluetooth) on a 6-point scale (1 = *not at all*, 6 = *very familiar*) (α = .71).

3.3. Qualitative analysis

Interview sessions were semi-structured, modified from seminal online and mobile studies (e.g., Campbell & Kelly, 2008; Hargittai, 2002). Participants were first asked to perform a few basic information privacy functions in mobile devices. Observations were made while the researcher refrained from influencing the respondents' actions. Follow-up questions were then asked in a prearranged but loosely structured order (see Appendix). The researcher took detailed notes at the conclusion of an individual session and analyzed them once all observations were completed. Participants were examined in terms of their (1) understanding and (2) routine skill sets, corresponding to the two main research questions of this study. The subtlety of the cognitive and behavioral responses was the key as the ultimate goal was to thread out commonalities of user privacy experiences in mobile use.

4. Results

4.1. Quantitative findings

Overall descriptive data indicated the extent to which the sampled young adult users from the African American community were equipped to make information privacy decisions in their mobile uses (RQ1). Table 2 shows the limited extent of privacy knowledge, despite some basic awareness among the participants (M = 3.55, SD = 1.66, total score = 7). Most respondents (84.7%) scored correctly on an item that asked about data collection capability by mobile services. However, this contrasted with each of the remaining items about institutional mobile data environments, of which less than a half of the respondents possessed understandings. For instance, only 18.6% were aware of the absence of any government policy restricting data retention by mobile app services. Furthermore, 42.4% of the participants also mistakenly believed that it is illegal for smartphone providers to collect locational data based on their mobile use.

The average skill score was very low (M = 20.28, SD = 6.86) out of a total of 42. The level of involvement in mobile-based information control was low for all five items concerning information privacy. A number of participants (33.9%) reported that they never turned off Wi-Fi for privacy concern, with as many as 13.6% reporting that they *never* changed default security setting of mobile or

Table 2
Distribution of mobile privacy literacy items.

Items	Measures	*M*	*SD*
Mobile privacy skill (1 = not at all, 6 = all the time)			
Information	Read a privacy policy of mobile apps, such as m-Facebook or Twitter	2.10	1.26
Information	Encrypt mobile phone and/or texting messages	2.22	1.64
Information	Change default security setting of mobile phone	3.84	1.64
Information	Turn off Wi-Fi for privacy	2.66	1.54
Information	Stop using a particular add-on service because you are afraid of disclosing personal data	2.98	1.57
Location	Turn off location service enabler for privacy or security concern	3.71	1.85
Location	Restrict a location based mobile service, such as Google Map or Restaurant Finder, because it is too sensitive	2.96	1.70
Mobile privacy knowledge (1 = correct, 0 = don't know and incorrect)			
Information	Most mobile apps, such as m-Facebook or m-Yahoo, monitor and record your browsing	0.84	0.36
Information	Companies today have the ability to place an ad that targets you based on information collected on your mobile phone	0.66	0.47
Information	When a mobile app has a privacy policy, it means the app will not share your information with other companies	0.42	0.49
Information	A mobile app service is legally allowed to share information about you with affiliates without telling you the names of the affiliates	0.33	0.47
Information	Government policy restricts how long mobile or smartphone service providers, such as Google Phone or iPhone, can store your personal data	0.18	0.39
Location	Carrying Cell Phones Give Law Authority The Ability To Track The Place You Go	0.52	0.50
Location	It is legal for your mobile or smartphone service provider, such as Apple (iPhone), to collect the location of you when you use mobile phone	0.57	0.49

Table 3
Predictors of mobile privacy literacy.

	Mobile privacy knowledge			Mobile privacy skill		
	b	*SE*	*p*	*b*	*SE*	*p*
Demographic factors						
Gender (female = high)	0.18	0.51	0.22	−0.19	2.05	0.22.
Age	0.06	0.14	0.68	0.11	0.58	0.45
Socio-economic factors						
HH income	0.37	0.20	0.01	−0.22	0.81	0.16
Parental education	−0.03	0.23	0.82	0.09	0.91	0.57
Mobile access						
Mobile Internet access	0.25	0.19	0.08	0.20	0.77	0.17
Mobile daily use	−0.00	0.05	0.99	−0.13	0.02	0.39
Mobile familiarity						
Basic mobile familiarity	0.09	0.04	0.49	0.32	0.18	0.03
Total R2 (%)		0.28			0.23	
Adjusted R2	0.15			.08		

Note: OLS multivariate regression was used. Entries are standardized coefficients.

smartphones. The low level of involvement was also found in the dimension of locational privacy. For instance, 22% of the participants reported that they *never* turned off location-service enabler for privacy reasons and over a half of them (57.6%) indicated that they rarely restricted the use of location-based mobile service.

Statistics from Table 3 display the predictive power of various social and technological determinants within the marginalized community in harnessing mobile-based information privacy knowledge and skill (RQ2). In the case of knowledge, regression analysis showed a significant difference based on income disparity – with more affluent participants more likely to be knowledgeable ($\beta = 0.37$, $p < .01$). There was no gender difference in both skill and knowledge levels. The frequency of mobile Internet access was positively associated with the level of knowledge ($\beta = 0.25$, $p < .05$).However, the intensity of mobile daily use was not a significant predictor of knowledge and skill levels. Likewise, basic mobile familiarity did *not* reach significance for mobile-based privacy knowledge. In the case of skill, none of the socio-demographic predictors were significant, while the positive and sizeable effect of basic mobile familiarity was found ($\beta = 0.32$, $p < .05$).

4.2. Qualitative findings

The overall typology of responses is summarized in Table 4. Almost all participants were quick to acknowledge the lack of awareness and skill from their parts, frustrated when confronted with assigned tasks. User frustration, however, was also confounded by an ill-conceived sense of personal control and functional confusion. Here the particularities of African American young users should be also taken into consideration. First, most of them used the mobile devices heavily to perform their daily informational activities. Still, such heavy reliance and other skills did not seem to have any clear impact on privacy-relevant tasks.

4.2.1. Functional confusion

When asked to perform specific tasks, users turned to a set of irrelevant functions. A common source of confusion was the mobile-Internet access. Some users misunderstood that the mobile device, even when they were accessing popular websites, was entirely different from the Internet. This was manifested through mischaracterization of mobile-Internet. One African American male respondent while trying to block Facebook mobile applications said, “I am more concerned about Internet than mobile, you know”. He went on to explain, “Mobile is more like inside, but Internet is way out there, you know . . ., wide and big”. The other respondent who indicated she liked to use twitter through mobile said, “If it was Internet and [if I now have] my computer, I could do it, but not with mobile”. This confusion between Internet access and mobile app access exacerbated a functional task of deleting cookies or history in web-related apps. “Can I do it with -iPhone?” One female user asked in response to the task of cookies. Other respondent bluntly admitted, “What is that?” “Hum, I don’t know. Actually, I’ve never done it”. An 18-year old female college student went to try to turn off Wi-Fi, adding “This does stop everything”.

The sentiment shared by others was that (1) mobile apps are separated from the Internet and (2) there is no distinction in digital platform among a phone device, mobile service provider, and mobile app. Even those who quickly found the policy statement

Table 4
Response typology of mobile privacy literacy.

	Observation	Typical user expression
1. Mobile privacy knowledge		
1.1. Functional confusion	Misuse or use of irrelevant functions; confusion over Internet vs. mobile; no distinction between mobile apps vs. mobile platform Privacy in immediate relationship	‘I don’t know’ ‘Can I do it?’ ‘Is it possible?’ ‘because cell phones are more close to me – it is smaller than wide internet’ ‘I can do it over internet, but not mobile’ ‘It is because of my girlfriend’ ‘I lock the phone all the time’
1.2. Familiar neglect	Familiar routine of not knowing; privacy setting eventually located; a sense of personalized control & misguided confidence	‘It must be in setting’ ‘Oh! here it is’ ‘Is this correct?’ ‘Am I doing right?’ ‘Touch-phone is easy’ ‘I can do it when I really need to’
2. Mobile privacy skill		
2.1. Use frustration	Embarrassment; giving up and acknowledgement; indignant about own mistake	‘Wow’ ‘I do not know this’ ‘I have to learn this’ ‘I have never done it’ ‘This is how I do!’

of a popular m-Twitter and performed basic functions admitted confusion. A 24-year-old African American male Blackberry user who worked for a local delivery service commented:

> Oh yes, I use my Blackberry all the time. Um, this is here. Maybe, too many options and keys ... If I don't pay attention to them, let's say it is really something new, yes I would not know them as a part of those settings until maybe I got to know them later or didn't feel like okay. I don't feel comfortable to share my personal life with them. I may take them out, but initially they were new to me, yea, I definitely would not know.

Another critical dimension of confusion during the interview process was that commercial data privacy was understood in the context of immediate relational surveillance. That is, the participants perceived mobile privacy in terms of close interpersonal issues, between boyfriends/girlfriends or parents/daughters. This was manifested particularly for location-specific privacy, as the concern often turned into the operation of irrelevant function such as locking mobile phone. A 20-year-old female user, when asked to adjust a locational setting of m-Twitter responded, "See . . . it's [my phone] locked", "I lock it all the time". Other male participant who indicated that he recently installed exercise (pushup) app emphasized the importance of locking phone "because no one else can use it without password". He went on to elaborate that it is "weird" not to lock the phone, "maybe because of my girlfriend".

4.2.2. Familiar routine of neglect

User confusion did not necessarily mean that they were incompetent in other functional tasks in their mobile uses. In fact, many participants eventually managed to locate privacy settings for a majority of assigned tasks. Moreover, nearly every respondent was adept at manipulating key functions of mobile devices – such as texting, online access, and browsing – almost instantly despite highly limited keypads and screen sizes. Such immediate fluency, however, was in sharp contrast with the fuzziness of personal information skill and knowledge operating in somewhat 'a familiar routine of neglect'. This refers to being familiar with most basic functionalities of mobile phones, but not being equipped with the understanding and ability to deal with issues of information privacy.

For instance, a 20 year-old African American female participant provided a typical response. When asked to find a location-service enabler, she mumbled, "It must be here in the setting . . .." "Um . . . oh my god, why is it not here? Um . . . Oh yes, here it is, I got it". Others needed reassurance, even when they were aware of basic locational-informational privacy functionalities. One participant who could not locate a location enabler quickly asked the investigator, "Am I doing it right?" One participant explained that she '*kind of always*' knew what to do but was '*not really self-conscious*' about it.

This somewhat fuzzy but familiar neglect (of what they think they knew) carried a sense of ill-conceived confidence and control. Moreover, commercial use of personal location or information rarely entered the minds of the young adult mobile users. The underlying dimension was the immediate confidence with which the participants felt that they could handle personal data in their mobiles easily when necessary. Interestingly, this premature sense of control was particularly pronounced among users of certain mobile devices, namely the latest iPhone, perhaps due to the easiness of touch screen functions. Moreover, the personalized nature of mobile phone use seemed to fuel this misguided confidence. A recent iPhone adopter who reported that he used mobile for 'everything' noted, "iPhone is very safe. And it is very easy to use . . . when I need to erase something, or do other stuffs". Another male participant elaborated, "iPhone's like a MAC, much more secure than a PC. Everything's integrated for consumers".

An 18 year old college freshman user also noted:

> Yes, it is very easy. But I just don't do much, though [Laugh]. I don't know, you know [A long pause]. Maybe because it is 'in' [Pointing at his pocket]. You know, I guess it is personal. And cause it's so easy, I'm not concerned and I can do when I really need to do.

Another user, a 22-year-old man who had a part-time job, provided a similar response, highlighting a sense of personalized control and immediate action for privacy that clearly contradicted his own skill and knowledge levels:

> It looks almost instant . . . to me with all touch screen characters. It's personal and I carry it all the time. I don't know. . . [Smiling]. I wouldn't know much. But it's readily available to do obvious things, visible, and just touch.

5. Discussion

This study adds to the existing knowledge in digital literacy literature by exploring different levels of knowledge and skills among younger adults from a marginalized community, as indicated by a set of questions that assessed mobile-based information and location privacy. Different analytical approaches of the two designs reflect distinct foci in triangulation. The purpose of the survey was to capture the overall contour of mobile literacy level and examine consequences of social and technological determinants. The in-depth observations allowed us to generate insights that could not be captured in the quantitative assessments of mobile skill and knowledge.

The two phases of the study complemented each other, providing further evidence of the value of a mixed-method. We found that overall levels of information-location privacy literacy were significantly low among young adults. Although some users took a limited set of actions to protect their privacy, most participants knew little about risk of information-location surveillance and could not perform simple privacy setting changes. Moreover, the users with lower parental income proved to be less knowledgeable than those with higher parental income. Low levels of mobile privacy skill persisted and privacy skill sets were predicted by basic mobile familiarity after accounting for other factors such as mobile Internet access and use.

In-depth interviews, accompanied by observations, added subtle dimensions – the extents of the lack of knowledge and skill were confounded by basic feature confusion, functional misunderstanding, and a sense of 'being personal' operating in a familiar routine of neglect. In-depth interview in fact shed light on how various forms of new digital data surveillance on mobile platforms were misunderstood. For instance, the users perceived that mobile use-access and online access are based on entirely different platforms for personal information dissemination. Further, many participants mistakenly believed new smartphones like iPhone worked best as data protection centers while focusing on an immediate circle of boy/girlfriends and acquaintances. Our findings from interview-observations help us identify the factors contributing to such insufficient levels of skill.

Taken together, the findings from this study have significant implications for digital literacy studies and information privacy policy related to mobile devices (see Humphreys et al., 2010). As the government policy continues to lag behind active legislations concerning location-information mobile surveillance, it is becoming more and more important to equip users with basic tools of cognitive skill sets to make informational decisions. Further, young adult mobile users will face increasingly complex decisions about institutionalized data markets and mobile app products. Yet their information knowledge seems dangerously inadequate for dealing with the complexity of digital data ecosystem (cf. Best, Taylor, Manktelow, & McQuilkin, 2014). It is also important to recognize that young adults from a low income background displayed particularly alarming low levels of knowledge. Rather, the influences of income, and other social determinants should be taken into account in public policy initiatives geared toward improving mobile-based digital literacy.

5.1. Particularities of African American community

Particularities of African American community should not be counted lightly. As of 2012, the broadband penetration rate of African American households continues to lag behind other communities, contrary to the explosion of mobile use. Thus, reliance on mobile devices in digital engagement for commercial, social, and political activities is exceptionally significant among African American young adults. A handful of studies (e.g., Zickuhr & Smith, 2012) documented the potential role of mobile phones in bridging the digital gap. While it can be true that mobile devices can be used to ease out the particular vulnerability of the disadvantaged social groups, the findings of our study suggest it may be also true that African American users may remain vulnerable or underprepared in responding to information privacy and potential pitfalls (Danna & Gandy, 2001).

In this regard, we are concerned that a relatively high level of mobile familiarity did not translate into mobile privacy knowledge. Likewise, the frequent daily mobile use was not significantly associated with privacy knowledge and skill. This contradicts the findings from recent online privacy studies that have shown positive associations between the frequency of online use and knowledge and skill levels (Park, 2013a; Park, 2013b). Yet the findings strongly suggest that mobile personal data ecosystem, perhaps even more than online, remains far from the public's commonsensical understandings and daily use. Accordingly, African Americans' heavy reliance on mobile phones appears to entail a serious social concern, rather than optimism. The critical point is not to deny the capacity of young people from underserved communities, but to point out the presence of barriers and the need of appropriate social and policy attention in enabling the full potential of the mobile phone as this serves as a primary platform of digital identities among younger and underserved populations.

This study's overall findings support the theoretical concern about the level of digital literacy (cf. Hargittai, 2002; Hargittai & Hinnant, 2008; Park, 2013a; Park, 2013b) among the 'digital natives' particularly at the second level of mobile privacy, as we concerned about those with socially underprivileged backgrounds. That is, the lack of mobile privacy skill, functional misunderstanding, and a premature sense of control suggest that mature grounds for mobile uses have not emerged yet and the benefits from the high penetration of the mobile among African Americans may need careful qualifications. Our thesis is that the concern over "the second-level" digital engagement remains true of increasingly connected mobile spheres, as serious quality issues persist among the young adult users – especially, those with the underprivileged backgrounds.

Here it is worthwhile to ask whether the low levels of mobile-based privacy knowledge and skill found in this study would be also prevalent among the young adults of other communities. This is a valid point to consider, given the rapid mobile adoption across all communities (Castells et al., 2007) and the personalized trend that accelerated data transaction in mobile use (Campbell & Park, 2008). In this regard, while we fully acknowledge the need for further studies, we also cautiously speculate that the absolute levels of knowledge and skill may remain limited among the 'digital natives' in general. In fact, there is a finding that despite the early adoption, the teenagers' mobile skill and use remained constrained with the limited consequences in their social engagements (Park, 2014). This, coupled with our study's findings, appears in line with other studies that indicated the complex decision process involving personal data disclosure (Humphreys, 2011; Humphreys et al., 2010) in the limited sets of skill related to online content creation (Hargittai & Hsieh, 2010; Litt, 2013). Still, to us, differences may reside in the extent to which the young African American users rely upon mobile devices as their dependence may complicate or even exacerbate privacy concern that we have for 'digital natives' in other communities (see Best et al., 2014). While we do not know the magnitude of such a difference, we are concerned that the societal backgrounds such as income gap continue to influence the readiness of privacy-related knowledge and skill even within the young mobile users from the same ethnic background.

6. Policy intervention

Given the levels of functional confusion and misunderstandings of 'a personalized sense of control' documented in this work, it becomes important to simplify the ways in which information privacy decisions can be made on mobile platforms is significant. For example, this study supports the basis of a study by Kahne, Feezell, and Lee (2012) that a digital literacy training aid to young mobile users, namely at the k-12 level, can foster effective participation in mobile apps and supplement stronger protective mobile privacy policy (cf. Park, 2011). Young adult mobile users considered in this study were disproportionately recent smartphone users who had accustomed to 'easy-to-use' touch screen in almost immediate functional skills (of other non-privacy related tasks) despite very low levels of mobile-based digital privacy literacy. Here again a particular attention is needed on the underserved communities with the lower income level because of their heavy reliance on mobile as an alternative to the broadband home connection. Collectively, this points to the need of promoting users' understandings as well as the functional easiness equipped in mobile devices, with particular sensitivity to the young adults from underserved populations.

The following measures are proposed. First, the findings suggest that a systematic government initiative should provide digital educational program that focuses on the basic locational and informational privacy literacy. Second, the FTC must devise and enforce clear guidelines for mobile service providers and advertising sectors to inform adult mobile users of their practices. Third, more fundamentally, the FTC in its broader digital literacy policy initiative must incorporate the need of young adult users from marginalized communities in early education. In sum, those measures can be concretized in:

(1) Federal training aid in local level digital literacy programs
(2) Standardization of mobile-apps privacy functionalities, and
(3) Targeted awareness program for young users, especially from minority segments

There can be alternative explanations in which education will be ineffective and also any regulatory mandate will create unnecessary burdens for mobile service vendors (Hoofnagle, King, Li, & Turow, 2010). However, privacy awareness should be understood as more incremental process that takes comprehensive intervention program over a period. Further, clear industry guidelines will help mobile app marketers tailor to mobile users' privacy concern and demand.

Granted the findings from this study should serve as a departure point for replication with bigger data sets, our mixed methods have advantages in exploring the nuanced conceptual understandings and mobile use in more depth. Note that some of significant regression results revealed clear influence of social determinant as shown in economic disparity, and at least this study's qualitative insights indicate that those inadequate levels of literacy do not appear negligible. Future studies should explore the potential mediating effects of (1) family digital environment and (2) social-psychological factors, with a focus on other underserved communities such as Latino or Asian-American mobile users. This appears an important next step of inquiry, given each community has different social and cultural dynamics that may have distinctive consequences in their mobile behaviors. Organizational settings of mobile-saturated workplace also entail in-depth studies of how the informed use and skill among employees will influence their readiness for effective digital participation. Finally, we did not consider privacy awareness and concern in its relationship with mobile-based social and political engagement among underserved user communities in our study, but this should be an important research question.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.chb.2014.05.041.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: awareness, information sharing, and privacy on the Facebook. *Proceedings of Privacy Enhancing Technologies Workshop (PET)*, Lecture Notes in Computer Science, Springer, 36–58.

Best, P., Taylor, B., Manktelow, R., & McQuilkin, J. (2014). Systematically retrieving research in the digital age: Case study on the topic of social networking sites and young people's mental health. *Journal of Information Science*, 0165551514521936.

Bosomworth, D. (2013). Mobile marketing statistics 2013. Retrieved September 5, 2009, from <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/>.

Brown, K., Campbell, S. W., & Ling, R. (2011). Mobile phones bridging the digital divide for teens in the US? *Future Internet, 3*(2), 144–158.

Burrell, J. (2010). Evaluating shared access: Social equality and the circulation of mobile phones in Rural Uganda. *Journal of Computer-Mediated Communication, 15*(2), 230–250.

Campbell, S. W., & Kelley, M. J. (2008). Mobile phone use among Alcoholics Anonymous members: new sites for recovery. *New Media & Society, 10*(6), 915–933.

Campbell, S. W., & Park, Y. J. (2008). Social implications of mobile telephony: The rise of personal communication society. *Sociology Compass, 2*(2), 371–387.

Castells, M., Fernandez-Ardevol, M., Qiu, J., & Sey, A. (2007). *Mobile communication and society: A global perspective*. Cambridge, MA: MIT Press.

Charski, M. (2004). Ad push to get Latinos wired to their cells. Marketing y Medios, October (1), 16–17.

Cottrill, C. (2011). Locational privacy: who protects? *URISA Journal-Urban and Regional Information Systems Association, 23*(2), 49.

Danna, A., & Gandy, O. (2001). All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Ethics, 40*, 373–386.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. (2001). Social implications of the Internet. *Annual Review of Sociology, 27*, 307–336.

FCC. (2002). Order declining to commence rulemaking to establish fair location information Practices. Retrieved September 5, 2009, from <http://www.epic.org/privacy/wireless/FCC_order.pdf>.

Franken, A. (2011). Letter to carrier IQ. Retrieved June 5, 2013, from http://www.forbes.com/sites/andygreenberg/2011/12/01/heres-the-letter-senator-al-franken-just-sent-to-phone-rootkit-firm-carrier-iq/.

FTC (2010). FTC staff issues privacy report, offers framework for consumers, businesses, and Policymakers. Retrieved September 5, 2013, from <http://www.ftc.gov/opa/2010/12/privacyreport.shtmS>.

FTC (2011). Consumer privacy and protection in the mobile marketplace. Retrieved Septemberm 5, 2013, from <http://www.ftc.gov/opa/2011/05/mobiletestimony.shtm>.

Grant, I.C. (2006). Online privacy: An issue for adolescents. Proceedings of the Child and Teen Consumption Conference, Copenhagen.

Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday, 7*(4).

Hargittai, E., & Hinnant, A. (2008). Digital inequality: Differences in young adults' use of the Internet. *Communication Research, 35*(5), 602–621.

Hargittai, E., & Hsieh, Y. L. P. (2010). Predictors and consequences of differentiated practices on social network sites. *Information, Communication & Society, 13*(4), 515–536.

Hoofnagle, C., King, J, Li, J., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? Retrieved September 5, 2013, from dx.doi.org/10.2139/ssrn.1589864.

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication, 61*(4), 575–595.

Humphreys, L., Gill, P., Krishnamurthy, B., & Newbury, E. (2010). Privacy on Twitter: how much is too much? Privacy issues on Twitter. *International Communication Association*, Retrieved September 5, 2013, from <http://www2.research.att.com/~bala/papers/ica10.pdf>.

Ito, M., et al. (2008). Living and learning with new media: Summary of findings from the digital youth project. The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, No. 52.

Kahne, J., Feezell, J., & Lee, N. (2012). Digital media literacy education and online civic and political participation. *International Journal of Communication, 6*, 1–24.

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29*(4), 1649–1656.

Litt, E., & Hargittai, E. (2014). Smile, snap, and share? A nuanced approach to privacy and online photo-sharing. *Poetics, 42*, 1–21.

Livingstone, S. (2007). Strategies of parental regulation in the media-rich home. *Computers in Human Behavior, 23*(3), 920–941.

Marx, G. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*, 369–390.

Park, Y. J. (2011). Provision of Internet privacy and market conditions: An empirical analysis. *Telecommunications Policy, 35*(7), 650–662.

Park, Y. J. (2013a). Digital literacy and privacy behavior. *Communication Research, 40*(2), 215–236.

Park, Y. J. (2013b). Offline status, online status: Reproduction of social categories in personal information skill and knowledge. *Social Science Computer Review, 31*(6), 680–702.

Park, Y. J. (2014). My whole world's in my palm! The second-level divide of teenagers' mobile use and skill. New Media & Society, 1461444813520302. Online First.

Park, Y. J., Campbell, S., & Kwak, N. (2012). Affect, cognition and reward: Predictors of privacy protection online. *Computers in Human Behavior, 28*(3), 1019–1027.

Pew Research Center. (2010). Social media and mobile Internet use among teens and young adults. Retrieved September 5, 2013, from <pewresearch.org/pubs/1484/social-mediamobile-internet-use-teens-millennials-fewer-blog>.

Skoric, M. M., Ying, D., & Ng, Y. (2009). Bowling online, not alone: Online social capital and political participation in Singapore. *Journal of Computer-Mediated Communication, 14*, 414–433.

Tombros, A., Ruthven, I., & Jose, J. (2005). How users assess Web pages for information Seeking. *Journal of the American Society for Information Science and Technology, 54*(4), 327–344.

Turow, J., Feldman, L., & Meltzer, K. (2005). Open to exploitation: American shoppers online and offline. Report of the Annenberg Public Policy Center, University of Pennsylvania, Philadelphia.

US census. (2011). Statistical abstract. Retrieved September 5, 2013, from <http://www.census.gov/prod/www/statistical_abstract.html>.

Zickuhr, K., & Smith, A. (2012). Digital differences. Retrieved September 5, 2013, from pewinternet.org/∼/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.