An Empirical Study on User Access Control in Online Social Networks

Minyue Ni
Software School
Shanghai Key Laboratory of Data Science
Fudan University
myni14@fudan.edu.cn

Yang Zhang
Faculty of Science, Technology and Communication
University of Luxembourg
yang.zhang@uni.lu

Weili Han
Software School
Shanghai Key Laboratory of Data Science
Fudan University
wlhan@fudan.edu.cn

Jun Pang
Faculty of Science, Technology and Communication
University of Luxembourg
jun.pang@uni.lu

ABSTRACT

In recent years, access control in online social networks has attracted academia a considerable amount of attention. Previously, researchers mainly studied this topic from a formal perspective. On the other hand, how users actually use access control in their daily social network life is left largely unexplored. This paper presents the first large-scale empirical study on users' access control usage on Twitter and Instagram. Based on the data of 150k users on Twitter and 280k users on Instagram collected consecutively during three months in New York, we have conducted both static and dynamic analysis on users' access control usage. Our findings include: female users, young users and Asian users are more concerned about their privacy; users who enable access control setting are less active and have smaller online social circles; global events and important festivals can influence users to change their access control setting. Furthermore, we exploit machine learning classifiers to perform an access control setting prediction. Through experiments, the predictor achieves a fair performance with the AUC equals to 0.70, indicating whether a user enables her access control setting or not can be predicted to a certain extent.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; H.2.8 [**Database Management**]: Database Applications—*Data mining*

Keywords

Online social networks; access control; empirical analysis; data mining

SACMAT'16, June 05-08, 2016, Shanghai, China

DOI: http://dx.doi.org/10.1145/2914642.2914644

1. INTRODUCTION

Online social networks (OSNs) have gained a huge success in the past decade. Leading players in the business including Facebook, Twitter and Instagram have attracted a huge number of users. Nowadays, OSNs have become a primary way for people to connect, communicate and share life moments. For instance, every day, 500M tweets are shared on Twitter, and Instagram users publish 60M photos[1]. OSNs have brought a lot of convenience to our life, users' privacy, on the other hand, has become a major concern due to the large amount of personal data shared online. Previously, researchers showed that a user's personal information can be inferred through statuses [18] and locations [25] that she shared in OSNs.

To mitigate users' privacy concern, major OSNs have deployed access control schemes to delegate the power to users themselves to control who can view their information. For example, Facebook provides a fine-grained access control scheme which enables users to apply different policies on each post they publish. Twitter and Instagram, on the other hand, provide a much simpler scheme. A Twitter or Instagram user could enable her access control setting such that strangers cannot have access to all detailed contents in her account, except for her profile picture, number of friends and number of online posts. To study and further improve access control in OSNs, academia have conducted many research, most of which take either formal or logical approaches. For instance, researchers have modeled access control with hybrid logic [11] and semantic web technology [3]. On the other hand, understanding how users exploit access control in their daily life is essential to improve access control in OSNs. Much to our surprise, this is left largely unexplored.

In this paper, we perform a large-scale empirical study on access control usage of Twitter and Instagram users in New York. To the best of our knowledge, this is the first work on analyzing users' access control on Twitter and Instagram. We collect data of 150k Twitter users and 280k Instagram users continuously within three months and study their access control usage from both static and dynamic point of view. Especially, the dynamic analysis is conducted on a daily base instead of a yearly base as done in previ-

[1]http://bit.ly/1Fij4er

ous works [8, 21]. This allows us to understand in depth how users exploit access control in their daily OSN life. Our contributions in this paper can be summarized as follows.

- We perform a static analysis on New York users' access control usage and find that female users and young users are more likely to enable their access control setting. Moreover, users who enable their access control setting tend to have smaller online social circles, but are more willing to conduct social activities in the offline world represented by location check-ins.

- We conduct a dynamic analysis on users' access control usage based on the three-month consecutive data. We find that a considerable amount of users change their access control setting frequently and there are more users (especially female users and young users) enabling their access control setting than disabling it. When users disable the access control setting, they tend to become less active online and delete some of their followers. Interestingly, we also find that important festivals and events cause more users to disable access control setting.

- We apply machine learning techniques to conduct a prediction on whether a user would enable her access control setting or not. By combining users' online behavior such as the number of followers, together with user demographics, our prediction experiments achieve a fair result in which the AUC (area under the ROC curve) equals to 0.70. This indicates a user's access control setting can be predicted to a certain degree.

The rest of the paper is organized as follows. Section 2 introduces background information of Twitter and Instagram's access control schemes as well as the dataset used for our study. Section 3 and Section 4 present static and dynamic analysis on users' access control usage, respectively. Section 5 performs an access control setting prediction using machine learning techniques. Section 6 discusses limitations of this paper. Section 7 summarises related work and Section 8 concludes the paper with some future works.

2. BACKGROUND AND DATASET

2.1 Access Control in OSNs

Facebook, Twitter and Instagram are among the most popular OSNs at the moment. By September 2015, Facebook has around 1.5 billion monthly active users with 83.5% of its users are outside the US and Canada[2], while Twitter and Instagram have 316 million and 400 million monthly active users respectively. Besides the difference in size, the three OSNs are also appealing to different demographics and usage. Facebook is a general purpose OSN[3] with users distributed more evenly to diverse ages, races and genders; Twitter on the other hand is largely treated as a news source, also its percentage of users with high education and income is higher than those of the other two OSNs; Instagram is a platform for users to share their life styles and its users are more skewed to young people.

[2]http://newsroom.fb.com/company-info/
[3]http://bit.ly/1OPYYwN

Access control schemes on these three OSNs are different as well. Facebook deploys a fine-grained access control scheme for users to control who can view their resources. This scheme is on a per-resource base, i.e., a user can define a specific access control policy for each of her photos and statuses. In addition, Facebook also introduces a function, namely friend list to help users categorize their friends into different lists, e.g., colleagues and family, and the organized friend lists can then be directly used in a user's access control policy which improves its access control scheme's usability. Different from Facebook, Twitter[4] and Instagram[5] provide users with a much simpler access control scheme. On Twitter and Instagram, users can only choose whether to enable their access control setting, i.e., protect their account or not. Once a user enables her access control setting, others who are not the user's approved followers cannot view any of her information except for her profile photo, number of followers/followees and number of posts. In the following analysis, we refer users who enable their access control setting as *private users* while others as *public users*.

To improve access control in OSNs, one important perspective is to understand how users apply their access control in their OSN life. Several previous works [12, 8, 21, 13] have focused on the access control usage on Facebook. However, to the best of our knowledge, there do not exist works focusing on Twitter and Instagram. As discussed above, these two OSNs deploy different access control schemes from Facebook. Therefore, it is important and meaningful to understand how users apply their access control setting on Twitter and Instagram to protect their privacy.

2.2 The Dataset

In this paper, we collect the access control usage data of New York users on Twitter and Instagram. Even though the dataset of New York users is not a random sample of the global population, due to the diversity of New York users [8], we believe that our analysis should be indicative enough to reflect users' access control usage in general.

To identify users in New York, we leverage check-ins (user-shared location information) on the two OSNs. Nowadays, many people use their OSN services on mobile devices, e.g., 80% of Twitter's active users are on mobile[6]. To adapt to this trend, major OSNs add new functionalities to their mobile versions, one of which is location sharing, namely check-in, through mobiles' GPS sensors. It is quite common for users to share a photo together with the location where the photo is taken. By exploiting check-ins to identify users in New York, we can ensure accurate results from our analysis. Moreover, it allows us to compare public and private users' mobility behaviors as well (see Section 3).

To obtain users' check-ins, we first define a geo-coordinate bounding box covering New York region and then exploit Twitter [16] streaming API[7] and Instagram REST API[8] to collect users' check-ins respectively. To make sure that the users are locals in New York rather than visitors, we only keep those users with more than 10 check-ins. Figure 1 depicts a sample of check-ins in New York on Instagram.

After identifying the users in New York, we use Twitter

[4]https://support.twitter.com/articles/14016
[5]https://help.instagram.com/116024195217477/
[6]https://about.twitter.com/company
[7]https://dev.twitter.com/streaming/overview
[8]https://www.instagram.com/developer/endpoints/

Table 1: Summary of the conducted analysis on Twitter and Instagram.

	Static analysis			Dynamic analysis			Prediction
	Demographics	Online	Offline	Demographics	Online	Global events	
Twitter	✓	✓	✓	✓	✓	✓	✓
Instagram			✓	✓		✓	

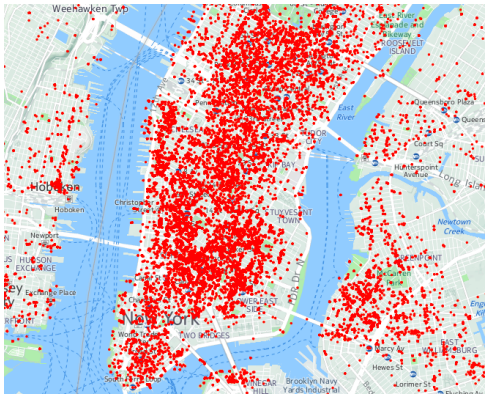


Figure 1: Check-ins in New York on Instagram.

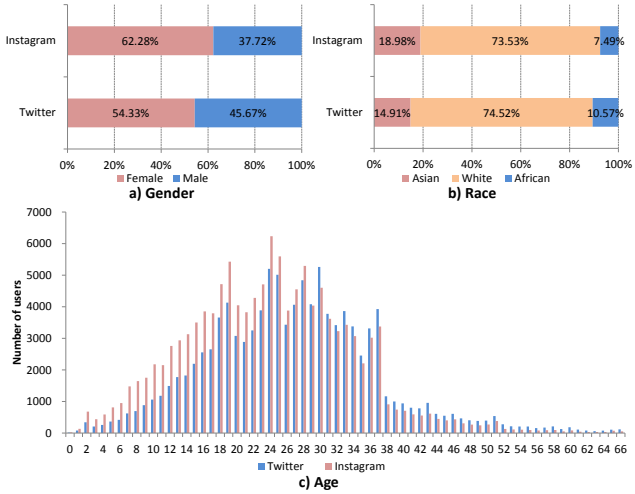


Figure 2: Gender, race and age distributions of New York users on Twitter and Instagram.

REST API[9] and Instagram REST API to extract users' access control setting together with some general information such as number of followers/followees and number of posts, on a daily basis for nearly three months, from October 15th, 2015 until January 12th, 2016. We regard accounts with more than 2,000 followers as celebrities and those whose followers are 1,000 more than followees as business accounts, and remove them from the dataset.

For static analysis, we focus on the data collected on November 12th with 175,202 users for Twiter and 292,406 users for Instagram[10]. For dynamic analysis, we focus on users that appear in our dataset everyday. In the end, we get 155,387 Twitter users and 282,066 Instagram users[11].

Note that when we exploit API to extract a private user's information, Twitter allows us to access the user's profile photo, number of followers/followees, and number of posts while Instagram forbids all the access. Since we get users' demographics through analyzing their profile photos, and quantify their online behavior through their numbers of followers/followees, and numbers of posts, we cannot conduct analysis related to those information on Instagram users. Table 1 lists the analysis we perform on the two OSNs.

Users' demographic information is another important aspect of our analysis. To get users' demographics, we resort to Face++[12], a state-of-the-art facial recognition service that detects a user's gender, race (Asian, White, African American) and age information from her profile photo. Face++ is based on deep learning techniques and has won several international competitions, it has also been exploited in other works for detecting users' demographics, such as [20, 19]. Figure 2 depicts gender, race and age distributions of our users on Twitter and Instagram. As we can see, there are more female users than male users on Twitter and Instagram in New York, and the proportion of female is much higher on Instagram. In addition, as mentioned before that Instagram attracts more young users than Twitter, thus its users' age distribution is skewed to younger ages than that of Twitter users.

3. STATIC ANALYSIS

In this section, we perform static analysis on users' access control usage. We start by checking the percentage of private users in our dataset, then analyze the relation between users' demographics and their access control usage. Users' online and offline behavior is discussed in the end. Here, a user's online behavior is quantified by her number of posts and followers/followees in OSNs, while offline behaviors are quantified by her mobility, i.e., check-ins. As mentioned in Section 2, we have no access to the demographic information and online bahaviors of private users on Instagram, thus we cannot perform static analysis on Instagram users' demographics and online behaviors.

3.1 General Statistic

As shown in Table 2, the general percentages of private users in our dataset are 5.22% for Twitter and 11.92% for Instagram. This indicates that Instagram users pay more attention to their privacy than Twitter users. The reason could be the different purposes of using the two OSNs (see

[9]https://dev.twitter.com/rest/public

[10]We have analyzed data collected on other dates and the analysis results are similar.

[11]Some users might delete their accounts or get suspended during the three months, thus the number of users for dynamic analysis is slightly smaller than the number of users used for static analysis.

[12]http://www.faceplusplus.com/

Section 2): Twitter is treated as a news spreading medium, thus its users are less likely to share personal sensitive information; Instagram, on the other hand, is a photo-sharing OSN and photos can contain personal sensitive information.

Table 2: Statistics of public and private users.

		General	With _Demo	Without _Demo
Twitter	Private	9,145 (5.22%)	6,066 (5.65%)	3,079 (4.54%)
	Public	166,057 (94.78%)	101,347 (94.35%)	64,710 (95.46%)
Instagram	Private	34,844 (11.92%)	- -	- -
	Public	257,562 (88.08%)	- -	- -

So far there does not exist official data from Twitter and Instagram on their private users' percentages. Cha et al. [5] claim that the percentage of private Twitter users is more than 7% which is close to our observation. The slight difference can be due to the sampling methodologies. The dataset in [5] is sampled through randomly picking user ids, while our dataset focuses on users in New York. On the other hand, the percentage of private users on Instagram is unclear from the literature. We emphasize that the focus of this paper is to understand how users exploit their access control in real life, the general percentages of private users on Twitter and Instagram are certainly interesting but left as future work.

3.2 Demographics

OBSERVATION 1: *Access control usage is different among users with different genders, races and ages. Female users, young users and Asian users are more likely to enable their access control setting than others.*

Gender. We calculate private users' percentages of male and female users respectively, and find out that more female users enable their access control setting than male users. As we can see from Figure 3, 4.15% of male Twitter users enable their access control setting while the corresponding rate of female users is 6.91%.

Race. Among people of three races in New York (see Figure 3), the private users' percentage of Asian users is the highest (6.20%) followed by White users (5.60%). African American users, on the other hand, have the lowest percentage (5.22%). One possible explanation could be the culture difference: Asian people are considered more conservative than White and African American people in general[13].

Age. Figure 3 shows that for all Twitter users who are older than 10, the percentages of private users are decreasing when the age grows. This trend is especially notable for users aged from 20 to 40, which indicates younger people are more concerned about their privacy than people of other ages. Interestingly, the private users' percentages of users under 10 years old (children) are high as well. Since children under 10 are less likely to be frequent Twitter users, we conjecture that these users use children's photos in their profiles.

[13]http://pewrsr.ch/1ccm9EL

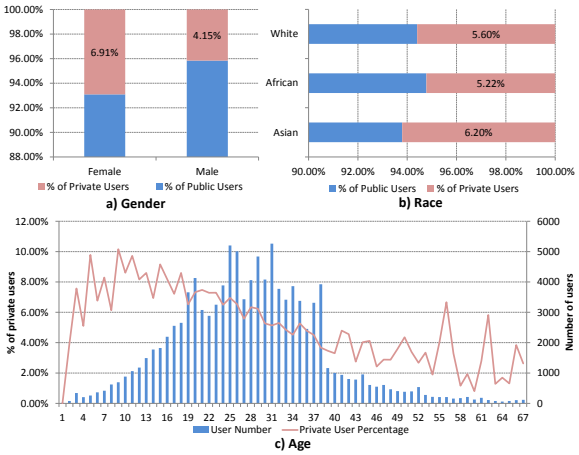


Figure 3: Demographic distributions of Twitter users.

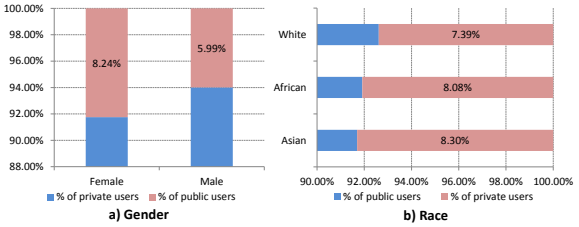


Figure 4: Demographic distributions of all users and users whose ages are below 10 on Twitter.

We further analyze users under 10 through their race and gender. Compared with Figure 3, Figure 4 shows that the percentages of private users have increased for both genders and all races. The percentage of female private users increases 1.33 percents to 8.24%, while that of male users increases 1.84 percents to 5.99%. Furthermore, Asian users remain to have the most private users, with the percentage of private users increases about 2.1 percents to 8.3%. Those two results coincide with the results in our analysis above that female users and Asian users are more concerned about their privacy. More importantly, we can see that users who use children's photos in their profiles tend to be more privacy-aware.

Profile pictures. As introduced in Section 2.2, we extract a user's demographic information through recognizing her profile photo with Face++. Therefore, if a user uses non-human pictures, such as a cat, in the profile, we cannot get her demographics[14]. Private users' percentages of Twitter users with and without demographics are listed in Table 2. Among 107,413 users with demographics, 6,066 (5.65%) users are private, while for 67,789 users without demographics, only 3,079 (4.54%) of them are private. This indicates that users without demographics (not using human photos) on Twitter care less about their privacy than those who use human pictures. The reason might be that using fake profile pictures makes users feel secure.

[14]By manually checking 100 users without demographics in our dataset, we find that more than 90% of these users use non-human pictures in their profiles.

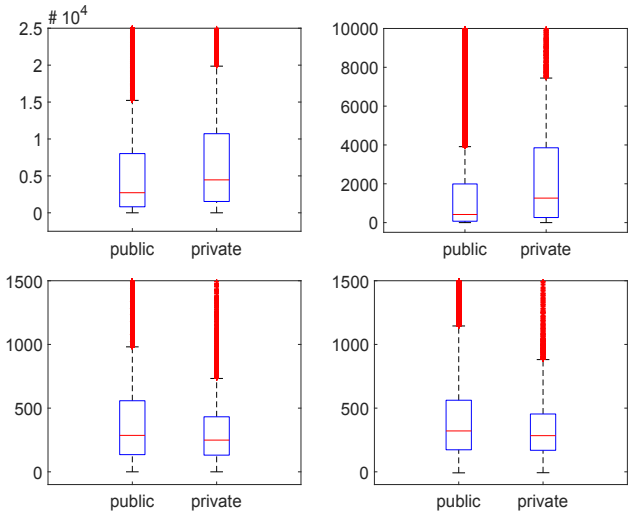


Figure 5: Users' distributions of posted tweets (top-left), favored tweets (top-right), followers (bottom-left) and followees (bottom-right).

3.3 Online Behavior

OBSERVATION 2: *Private users share more contents but have smaller online social circles than public users.*

Four metrics are exploited to quantify a Twitter user's online behavior, including the number of posted tweets, the number of favorites, the number of followers and the number of followees. The former two metrics can be used to evaluate the active level of each user on Twitter, while the latter two represent the size of each user's social circle.

We use box plots [23] to visualize the distributions of four metrics for private and public users respectively (see Figure 5). Box plot, i.e., box and whisker diagram, is a standardized way of displaying data distribution based on the five number summary: minimum, first quartile (25%), median, third quartile (75%), and maximum.

From Figure 5, we observe that, compared with public users, private users have published and favored more tweets. On average, private users have posted 8,864.07 tweets and favored 3,380.43 tweets, while public users posted 7,550.96 tweets and favored 2,277.58 tweets. There are two possible explanations for this result:

- Private users publish more tweets, i.e., to express themselves, since they are aware that their privacy is guaranteed to a certain extent;
- Users who have used Twitter for a longer period of time are more likely to become private since they are more aware of the privacy threats. Meanwhile, their longer Twitter-ages result in more tweets.

In Section 4, we perform further analysis on this from a dynamic point of view.

Public users have more followers and followees than private users (see Figure 5). On average, public users have 423.26 followers and 431.73 followees, while private users have 329.37 followers and 355.17 followees. This indicates that private users have much smaller social circles. Fewer followers may due to Twitter's access control scheme since private users have to give approvals to their followers. On the other hand, private users following less people is an interesting observation. This suggests that private users tend to filter not only their followers, but also followees to ensure their social circles to be less chaos.

3.4 Offline Behavior

OBSERVATION 3: *Private users are more socially active than public users in the offline world.*

The mobility data we get from Twitter and Instagram can be a good reflection of New York users' offline life. Our mobility dataset is composed of users' check-ins, and each check-in of a user tells us when and where the user is. In the following, we conduct our analysis from these two aspects.

Time. Figure 6 depicts the distributions of users' check-in time on a daily base on Twitter and Instagram. Despite the different distribution curves (Twitter users are more active at late night and early morning), we can observe an agreement between the two OSNs: compared to public users, private users are more active at night. As most offline social activities happen at night rather than working hours, this indicates that private users are more socially active in the offline world.

Locations. Due to the different designs of the two OSNs' APIs, we can extract the category information of each location for Instagram while not for Twitter. Here, location category information on Instagram is from Foursquare, a popular location-based social network, in which different location categories are organized into a tree structure[15]. In this paper, we take the first layer of the category tree (nine categories) to label each location, including entertainment, university, food, nightlife, outdoor, professional, residence, store and transportation.

Figure 7 depicts distributions of public and private users' check-ins over different location categories. It shows that private users have more check-ins at food and nightlife places. Since many offline social activities happen at these two types of places, this further confirms that private users are more active in the offline world.

3.5 Summary

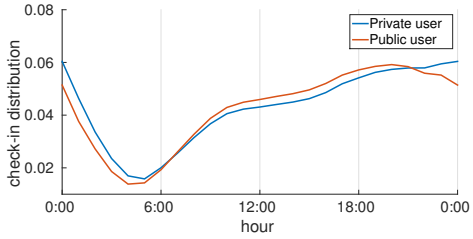
Our static analysis focuses on three aspects including demographics, online behavior and offline behavior. We have observed that:

- Female users, young users and Asian users are more concerned about their privacy than others;
- Private users publish more posts than public users, but have smaller online social circles;
- In the offline world, private users are more socially active than public users.

4. DYNAMIC ANALYSIS

After the static analysis, in this section we study New York users' access control usage from a dynamic perspective. Questions we attempt to answer include: how many users have changed their access control setting; what is the changing trend; who are these users; what is the correlation between users' changing of access control and other factors such as online behavior and global events?

[15]https://developer.foursquare.com/categorytree



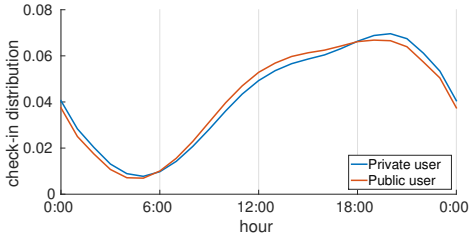


Figure 6: Check-in distribution over time on Twitter (left) and Instagram (right).

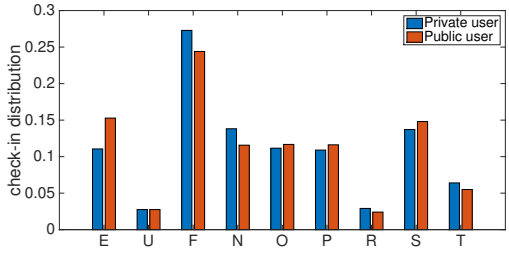


Figure 7: Check-in distributions over location categories on Instagram, each category is represented by its first letter, e.g., F stands for food.

We start by checking the general statistics of users who change access control setting, then focus on these users' demographics. Next, the correlation between access control changes and users' online behavior is analyzed. In the end, we study the influence from global events and festivals on users' decisions of changing access control.

4.1 General Statistics

Observation 4: *A considerable amount of users' access control usage is dynamic, i.e., they change their access control setting from time to time. There are more users changing their access control setting from public to private than from private to public.*

Changing frequency. A considerable amount of users in our dataset have changed their access control setting during the three months. On Twitter, 7,590 (5.21% of total Twitter users) users have changed their access control setting, while the proportion on Instagram is much higher (19.95% of 56,261 users).

Table 3 further presents the statistics of times that users have changed their access control setting. Among all the Twitter users who have changed their access control, 54.44% of users have changed more than once. On the other hand, Instagram users seem to be more indeterminate on access control usage: 69.09% of them have changed more than once during the three months. Moreover, 553 Instagram users have even changed more than 15 times.

Changing trend. From the dataset, we have observed an increasing trend of users enabling their access control setting during the three months, i.e., more users change from public to private than changing from private to public. On October 14th 2015, 4.89% of Twitter users and 9.36% of Instagram users in our dataset are private, while on January 12th 2016, the percentages have increased to 5.62% on Twitter and 14.20% on Instagram. This result indicates that users' privacy concerns are increasing day by day. Note that similar reslts are obtained for New York [8] and Pittsburgh [21] users on Facebook.

Table 3: Statistics of users' changing frequency.

Times Changed	Twitter User	% of Users	Instagram User	% of Users
1	3,458	45.56%	17,390	30.91%
2	2,494	32.86%	15,252	27.11%
3	473	6.23%	4,397	7.82%
4	506	6.67%	5,179	9.21%
5	171	2.25%	2,121	3.77%
6	153	2.02%	2,597	4.62%
7	83	1.09%	1,220	2.17%
8	59	0.78%	1,470	2.61%
9	44	0.58%	849	1.51%
10	39	0.51%	955	1.70%
11	20	0.26%	552	0.98%
12	23	0.30%	721	1.28%
13	11	0.14%	455	0.81%
14	12	0.16%	493	0.88%
15	5	0.07%	267	0.47%
>15	28	0.51%	553	4.16%
Total	7,590		56,261	

4.2 Demographics

Observation 5: *Female users and young users change access control setting more frequently and have a faster changing trend from public to private than others. White users change access control setting least frequently and their changing trend from public to private remains the slowest.*

Changing frequency and demographics. The statistics of both Twitter and Instagram[16] users' changing frequency w.r.t. demographics is presented in Table 4, 6.52% of female users and 3.66% of male users on Twitter, and 19.20% of female users and 13.92% of male users on Instagram have changed their access control setting. In addition, female users change access control more frequently than male users. Especially on Instagram, the average changing times for female users is 3.60, while it is 2.93 for male users.

On Twitter, Asian users have the highest proportion of access control changing (6.11%), while African American users have the most frequent changing times, i.e., 2.40 times on av-

[16]As some public users with demographics on Instagram change their access control setting to private during the three months, we can still study Instagram users' changing frequency and trend w.r.t. demographics here.

Table 4: Statistics of users' changing frequency on Twitter and Instagram w.r.t. demographics.

			Gender		Race			Age			
		General	F	M	Asia	Africa	White	0-10	11-30	31-45	>46
Twitter	users changed (%)		6.52	3.66	6.11	5.16	5.04	7.72	5.95	3.29	2.41
	average changed times	2.29	2.37	2.09	2.37	2.40	2.25	2.52	2.28	2.23	2.07
	users changed once (%)	45.59	43.77	49.44	42.28	42.14	46.89	41.15	44.77	51.23	48.45
Instagram	users changed (%)		19.20	13.92	19.33	20.63	16.32	20.19	18.09	13.14	11.34
	average changed times	3.40	3.60	2.93	3.84	3.78	3.22	3.74	3.47	2.82	2.90
	users changed once (%)	34.85	31.68	42.08	27.79	30.53	37.55	32.26	33.26	43.63	46.71

erage. On the other hand, 20.63% of African American users have changed their access control setting on Instagram, but Asian users have the most changing times, 3.84 on average. On both Twitter and Instagram, White users are the most determinate about their access control setting.

We discretize age into four bins and study users' changing frequency w.r.t. each age bin. On both Twitter and Instagram, younger users change their access control setting more frequently. For instance, 18.09% Instagram users between 11 and 30 years old have changed at least once and the average changing times is 3.74. While for users between 31 and 45 years old, the two number is 13.14% and 2.82 respectively. In addition, users under 10 is the group with the highest number of users who change their access control setting freqently, this is consistent with our previous analysis that users under 10, i.e., users using children's photos in their profiles are more concerned about their privacy.

Changing trend and demographics. We further study the changing trend of users w.r.t. demographics. As shown in Figure 8a), female private users' percentage grows faster than that of male users. On Twitter, the percentage of private female users increases 0.94%, while that of private male users is 0.72%. This trend is more obvious on Instagram, private female users' percentage increases nearly 10% while private male users' percentage increases about 8%.

Trends of enabling access control setting by users of different races are exhibited in Fig. 8b). On Twitter, the proportion of private African American users increases the slowest, while on Instagram, it becomes the fastest. We believe it is caused by the different purposes of the two OSNs.

The changing trend for users of different age (bin) is plotted in Fig. 8c). On both Twitter and Instagram, the private users' percentage of younger users increases faster than older users. This accords with the result in Section 3 that young users are more concerned about their privacy.

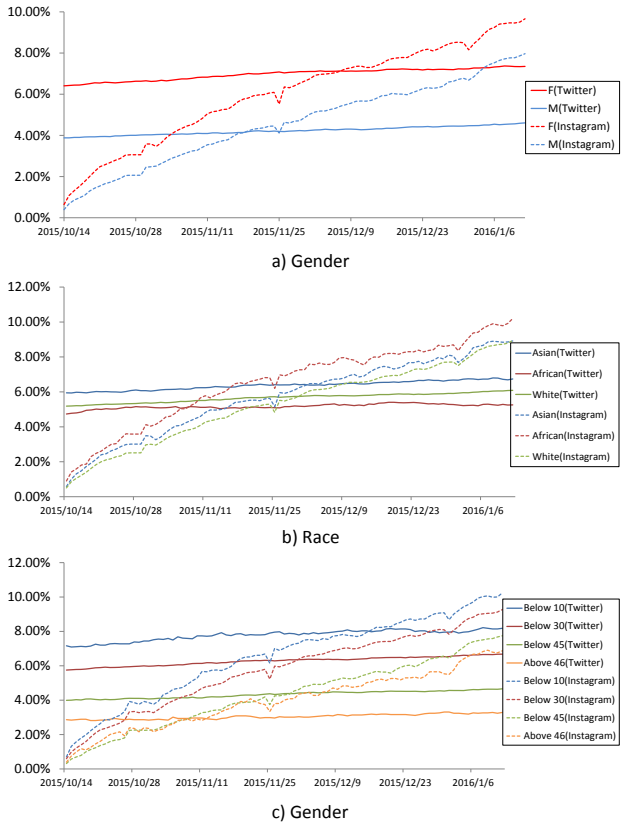


Figure 8: Changing trends of proportions of private users based on their demographics in our dataset. As we cannot get private users' demographics from Instagram in the beginning, thus the beginning proportion for Instagram users w.r.t. different demographics is approaching 0.

4.3 Online Behavior

Observation 6: *In general, users being private through all the three months and users changing from public to private tend to be less active in publishing new contents. Besides, these users barely establish new relationships with others, and their followers become fewer. Moreover, topics of users' posts on both OSNs are more (less) personal/sensitive when changing from public (private) to private (public).*

Statistics of online behavior. We first refer users staying private (public) within the three month as *constantly-private* (*constantly-public*) users, users who have changed their access control setting are named *inconstant users*. Based on users' online behavior presented in Section 3, we design four metrics to evaluate users' dynamic online behavior, including 1) new tweets; 2) new favorites; 3) new followers; and 4) new followees, added daily[17].

The comparisons between the constantly-public users and constantly-private users w.r.t. four metrics of dynamic online behavior are shown in Figure 9. Recall the observation in Section 3 that private users have more tweets (and favored tweets) than public users in general. Here, we find

[17]Different from demographics, users' online behaviors are dynamic, for instance, number of followers may vary everyday. Thus, we cannot apply the same method for demographics to analyze Instagram users' dynamic online behavior in this section.

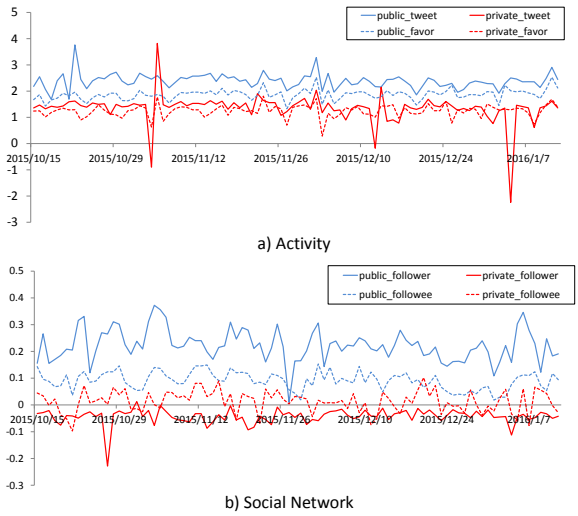


Figure 9: Constantly-public and constantly-private users daily added new tweets, favored tweets, followers and followees.

that, on the contrary, constantly-private users have less new and favored tweets everyday than constantly-public users on average. In Figure 9a), both curves representing constantly-private users are below the ones for constantly-public users. In Section 3, the two explanations why private users having more tweets than public users include: users are more comfortable to express themselves in the private context; private users have longer Twitter-ages, thus having more tweets. The result in Figure 9a) gives a strong support for the second explanation, i.e., longer Twitter-age is the reason why private users have more Tweets than public users.

We also find that constantly-private users barely establish new links with others, i.e., their average amount of daily new followers and followees are very close to 0, while constantly-public users often have new followers and followees every day. This suggests that private users are more careful on choosing their followers and followees (similar to the summary in Section 3).

Inconstant users' dynamic online behavior statistics are presented in Table 5. It appears that users changing from public to private have fewer newly posted and favored tweets than those changing from private to public. Moreover, inconstant users changing from public to private are reducing their followers and followees. In addition, more followers are deleted than followees (-0.15 vs. -0.04), which indicates that users' one purpose of enabling access control is, to some extent, to protect themselves from being viewed by someone from whom they are hiding sensitive information. In another way, users are more concerned about privacy leakage through who follows them than who they follow. This result reflects some fundamental differences between follower and followee relations on Twitter.

User topics. Next, we analyze posts (tweets for Twitter and captions of photos for Instagram) that users publish before and after they change access control setting and check whether topics of users' posts have changed.

We exploit a classical topic modeling algorithm in the natural language processing field, namely Latent Dirichlet Allocation (LDA) [1] to detect topics from users' posts. We

Table 5: Statistics of inconstant users' dynamic online behaviors.

	Public to private	Private to public
Tweets	3.12	5.64
Favorites	4.35	4.67
Followers	-0.15	0.25
Followees	-0.04	0.14

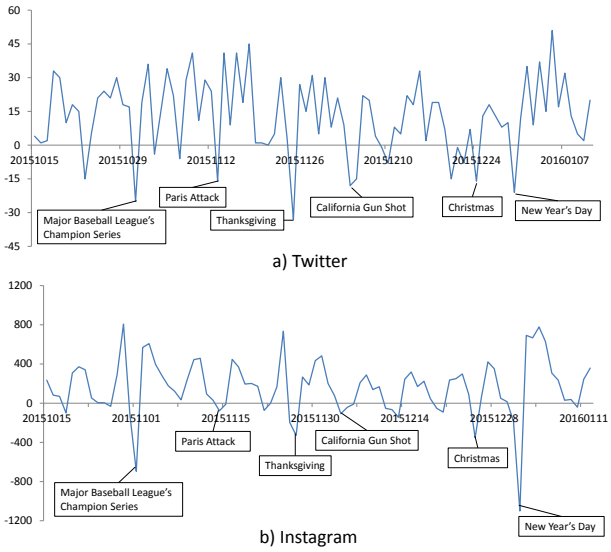


Figure 10: Differences between daily new private users and daily new public users.

start to query each inconstant user's posts through the corresponding API one day before and after she changed her access control setting, then aggregate posts of each user together as one document. Punctuations and stop words are filtered out during the process. We then organize all the documents into a corpus, and remove words that appear in less than 20 documents and more than 70% of the documents [24]. Note that for users who change from public to private, we cannot get their published posts on both Twitter and Instagram. However, as users frequently change their access control setting and some private users become public on the day we collect their published posts (January 21, 2016), we are able to extract topics from their posts when they change from public to private.

Table 6 lists the top 3 topics for Twitter and Instagram when users change their access control setting. We observe that when users are public, their topics are not privacy-sensitive, for instance, "happy, years, new" published during the New Year on Twitter and "follow, keep, coming" representing the popular hashtags on Instagram. On the other hand, when users enable their access control setting, their topics become more private, such as "family" on Twitter and "missing" on Instagram.

4.4 Global Events and Festivals

OBSERVATION 7: *Global events and festivals cause more users to change access control setting from private to public.*

As stated before, the trend for users to enable their access control setting is increasing, thus there should be more users

Table 6: Topics of users' posts one day before and after changing their access control settings.

Twitter	Public to private		Private to public	
	before	after	before	after
Topic 1	happy years new	woman get never	just one time	can party still
Topic 2	music nothing three	family made truth	person every crying	one just kids
Topic 3	nice looking needs	like boys text	bitch whole one	team really win
Instagram	**Public to private**		**Private to public**	
	before	**after**	**before**	**after**
Topic 1	follow keep coming	thankful already missing	good morning feeling	god person remember
Topic 2	go let strong	feels puppy wake	come show true	inspiration goodnight sleep
Topic 3	can't wait next	get also link	family friends lit	art music yesterday

changing from public to private than from private to public every day. However, when plotting the difference between daily new private users and public users (the number of new private user subtracts the number of new public users), we have found several interesting dates on which many more users changed from private to public than from public to private (see Figure 10).

On three important festivals in the US, i.e., Thanksgiving (November 26th, 2015), Christmas (December 25th, 2015) and New Year's Day (January 1st, 2016), more users disable their access control setting on both Twitter and Instagram. This indicates that on holidays, users are more open and less concerned about their privacy for the purpose of meeting new people and expressing gratitude.

In addition, we find that some global events might cause more people to become public in OSNs as well. For instance, more users become public on November 13, 2015 (Paris terrorist attack) and on December 3rd, 2015 (California gun shot case). This is probably because users are more willing to express their opinions when such events take place.

There also exists an obvious drop on November 1, 2015 on both OSNs, we believe this is due to the final match of the Major Baseball League's champion series between New York Mets and Kansas City Royals held in New York. Even though New York Mets lost the championship on that day, there are still New York users becoming public to communicate with other baseball fans on Twitter and Instagram.

4.5 Summary

In this section, we study dynamic usage of users' access control in OSNs and have observed the following.

- Many users change their access control setting from time to time. Instagram users change more often than Twitter users. More users change from public to private, showing that users become more concerned about their privacy day by day.

- Female users and young users change their access control setting more frequently and their changing trend from public to private is faster than others. Asian and African American users behave differently on Twitter and Instagram, while White users' changing behavior is the least active on both OSNs.

- Constantly-private users are less active than constantly-public users in terms of published posts and new followers/followees. When users change from public to private, they publish less tweets than users changing from private to public, and delete their followers, their posts' topics are more privacy-sensitive than before.

- Global events and festivals cause more users to change access control setting from private to public.

5. ACCESS CONTROL PREDICTION

After analyzing users' access control usage, in this section we investigate whether it is possible to predict a user's access control setting. Being able to predict a user's access control setting opens up opportunities for appealing applications. For instance, OSNs can automatically assign access control setting to their users for better privacy protection; government can develop a privacy advisor to remind users of their privacy leakage. Our prediction is based on users' static information, by only using a user's information listed on the OSN page, we aim to predict whether the user should enable access control setting or not.

We model access control prediction as a binary classification problem, and intend to solve the problem with machine learning classifiers. We label private users as positive cases while public users as negative cases. For features used in classification, two models are constructed, namely Model1 and Model2. Model1 exploits users' static online behavior including number of followers/followees, number of tweets and number of favorites as features for classification. Model2 combines the features of Model1 with demographics. In demographics, there are two categorical variables including gender and race, we change them into dummy variables for classification. Three machine learning classifiers, i.e., logistic regression, random forest and gradient boosting, have been used to conduct prediction. ROC (Receiver operating characteristic) curve and AUC (area under the ROC curve) are used as evaluation metrics.

Table 7: AUC of prediction.

	Model1	Model2
logistic regression	0.59	0.62
random forest	0.61	0.64
gradient boosting	0.69	0.70

Table 7 lists the AUC for two models under each classifier. Our best prediction result (gradient boosting and

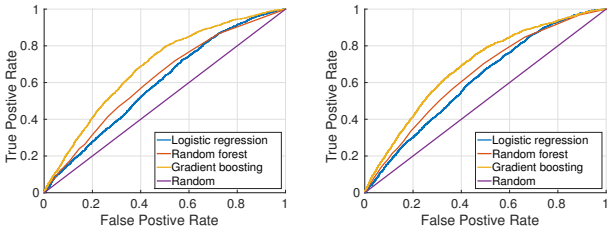


Figure 11: ROC curves for `Model1` (left) and `Model2` (right) w.r.t. different classifiers.

Model2) is fair, the AUC equals to 0.70[18], which indicates that users' access control setting can be predicted to a certain extent. Model2 achieves a better result than Model1 indicating demographics' usefulness on separating public and private users. Figure 11 further depicts the ROC curves for Model1 and Model2, respectively.

As we cannot get private users' demographics and online behavior information from Instagram's API (see Section 2), we only focus on Twitter users for access control prediction.

6. LIMITATIONS

In this section, we discuss a few limitations in our study.

Dataset. The current work focus on New York users' access control usage. Even though the user sample is large (more than 150k users for Twitter and and more than 280k users for Instagram), there still exist some region bias in our analysis. Meanwhile, knowing users being in New York allows us to conduct some more interesting analysis, such as users' offline behaviors (see Section 3) as well as a base ball match's influences on users' access control changing (see Section 4).

Social relation and access control. Section 4 concludes that when a user changes her access control setting from public to private, the user is more likely to reduce her number of followers. However, we haven't conducted the detailed analysis on who are these users being deleted. One obstacle for this analysis is the restriction of the API: Twitter allows much less access to their users' social networks[19], while Instagram provides only a small number of followers/followees of a user each time[20].

7. RELATED WORK

Access control in OSNs has attracted academia a considerable amount of attention during the past decade. Many researchers have focused on modeling access control schemes in OSNs from a formal or logical perspective. Carminati et al. [4] propose three regulations for access control scheme in OSNs, including social relation, distance in social network as well as trust level. The authors of [10] describe a two-stage access control where, to access a resource of a certain user, one has to be able to reach that user in the social network and then requests the access. Besides modeling access control schemes, researchers have also proposed methods to precisely define access control policies. In [3], access control policies are defined by semantic web technologies. The authors of in [9, 2] propose to use hybrid logic as the policy language, this logic has been demonstrated quite powerful and later be used in several works including [22, 7, 14, 17, 6, 15].

Compared to the formal perspective, not many works focus on the empirical perspective of access control in OSNs. Existing works include [12, 8, 21, 13]. Compared to these works, this paper has the following advantages:

- We perform dynamic analysis on users' access control usage within three consecutive months, which allows us to study users' change from a daily perspective and provide with more insightful conclusion on users daily online activities. On the other hand, the dynamic analysis in [8, 21] is yearly-based, which can only provide a general trend of access control usage. For instance, the authors of [21] study users' access control setting once a year from 2005 to 2011 and discover that more and more Facebook users in Pittsburgh enable their access control setting every year.

- This paper conducts a much more comprehensive study than previous ones ranging from users' demographics to online behavior. Besides, we are the first to analyze the relation between access control and users' offline behaviors (mobility information), topics of published texts and global events.

- This paper is the first to show that it is possible to use users' information to predict their access control setting to a certain extent. This result can potentially lead to promising applications such as automatic access control enforcement and privacy advisor.

- Our user sample is bigger than most of the previous works. We have more than 150k users for Twitter and more than 280k users for Instagram while the dataset in [12] focuses on 200 users and the one in [21, 13] has around 1,000 users. On the other hand, the authors of [8] use a bigger sample than us (1.4 million New York users on Facebook).

Besides the above advantages, all of [12, 8, 21, 13] only focus on Facebook while, to the best of our knowledge, this is the first work to analyze users' access control usage on Twitter and Instagram. As stated in Section 2, Twitter and Instagram have different types of users and functions compared to Facebook, thus it is very interesting and meaningful to study their users' access control usage.

8. CONCLUSION AND FUTURE WORK

We have conducted the first large-scale empirical study on users' access control usage on Twitter and Instagram. Our analysis focused on both static and dynamic perspectives. We further demonstrated that users' access control setting can be predicted to a certain extent.

For the future work, we plan to conduct analysis on other cities to check whether culture differences play a role in users' access control usage. Our access control prediction is only based on users' static information, we plan to explore users' dynamic information to predict whether a user will change her access control setting on a certain day by using more sophisticated features in machine learning classifiers.

[18]AUC is not sensitive to label imbalance problem and AUC for random guessing is around 0.5.

[19]https://dev.twitter.com/rest/public/rate-limiting

[20]https://www.instagram.com/developer/endpoints/relationships/

Acknowledgement

Minyue Ni and Weili Han are supported by NSFC (Grant No. 61572136). We thank anonymous reviewers for their comments.

References

[1] D. Blei, A. Ng, and M. Jordan. Latent dirichlet allocation. *Journal of Machine Learning Research*, 3:993–1022, 2003.

[2] G. Bruns, P. W. L. Fong, I. Siahaan, and M. Huth. Relationship-based access control: its expression and enforcement through hybrid logic. In *Proc. 2nd ACM Conference on Data and Application Security and Privacy (CODASPY)*, pages 117–124. ACM, 2012.

[3] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. A semantic web based framework for social network access control. In *Proc. 14th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 177–186. ACM, 2009.

[4] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In *Proc. IFIP WG 2.12 and 2.14 Semantic Web Workshop (OTM)*, volume 4278 of *LNCS*, pages 1734–1744. Springer, 2006.

[5] M. Cha, H. Haddadi, and F. B. K. P. Gummadi. Measuring user influence in Twitter: The million follower fallacy. In *Proc. 4th AAAI Conference on Weblogs and Social Media (ICWSM)*, pages 10–17. The AAAI Press, 2010.

[6] M. Cramer, J. Pang, and Y. Zhang. A logical approach to restricting access in online social networks. In *Proc. 20th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 75–86. ACM, 2015.

[7] J. Crampton and J. Sellwood. Path conditions and principal matching: a new approach to access control. In *Proc. 19th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 187–198. ACM, 2014.

[8] R. Dey, Z. Jelveh, and K. Ross. Facebook users have become much more private: A large-scale study. In *Proc. 2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 346–352. IEEE, 2012.

[9] P. W. L. Fong. Preventing sybil attacks by privilege attenuation: a design principle for social network systems. In *Proc. 32nd IEEE Symposium on Security and Privacy (S&P)*, pages 263–278. IEEE CS, 2011.

[10] P. W. L. Fong, M. M. Anwar, and Z. Zhao. A privacy preservation model for Facebook-style social network systems. In *Proc. 14th European Symposium on Research in Computer Security (ESORICS)*, volume 5789 of *LNCS*, pages 303–320. Springer, 2009.

[11] P. W. L. Fong and I. Siahaan. Relationship-based access control policies and their policy languages. In *Proc. 16th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 51–60. ACM, 2011.

[12] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing Facebook privacy settings: user expectations vs. reality. In *Proc. 2011 ACM SIGCOMM conference on Internet measurement conference (IMC)*, pages 61–70. ACM, 2011.

[13] M. Mondal, Y. Liu, B. Viswanath, K. P. Gummadi, and A. Mislove. Understanding and specifying social access control lists. In *Proc. 10th Symposium on Usable Privacy and Security (SOUPS)*, pages 271–283. USENIX Association, 2012.

[14] J. Pang and Y. Zhang. A new access control scheme for Facebook-style social networks. In *Proc. 9th Conference on Availability, Reliability and Security (ARES)*, pages 1–10. IEEE CS, 2014.

[15] J. Pang and Y. Zhang. Cryptographic protocols for enforcing relationship-based access control policies. In *Proc. 39th Annual IEEE Computers, Software & Applications Conference (COMPSAC)*, pages 484–493. IEEE CS, 2015.

[16] J. Pang and Y. Zhang. Location prediction: communities speak louder than friends. In *Proc. 3rd ACM on Conference on Online Social Networks (COSN)*, pages 161–171. ACM, 2015.

[17] J. Pang and Y. Zhang. A new access control scheme for Facebook-style social networks. *Computers & Security*, 54:44–59, 2015.

[18] M. J. Paul and M. Dredze. You are what you tweet: Analyzing twitter for public health. In *Proc. 5th AAAI Conference on Weblogs and Social Media (ICWSM)*, pages 265–272. The AAAI Press, 2011.

[19] M. Redi, D. Quercia, L. Graham, and S. Gosling. Like partying? your face says it all. Predicting the ambiance of places with profile pictures. In *Proc. 9th AAAI Conference on Weblogs and Social Media (ICWSM)*, pages 347–356. The AAAI Press, 2015.

[20] F. Souza, D. de Las Casas, V. Flores, S. Youn, M. Cha, D. Quercia, and V. Almeida. Dawn of the selfie era: The whos, wheres, and hows of selfies on Instagram. In *Proc. 3rd ACM on Conference on Online Social Networks (COSN)*, pages 221–231. ACM, 2015.

[21] F. Stutzman, R. Gross, and A. Acquisti. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, 4(2):2, 2013.

[22] E. Tarameshloo, P. W. L. Fong, and P. Mohassel. On protection in federated social computing systems. In *Proc. 4th ACM Conference on Data and Application Security and Privacy (CODASPY)*, pages 75–86. ACM, 2014.

[23] J. W. Tukey. *Exploratory Data Analysis*. Pearson, 1977.

[24] W. X. Zhao, J. Jiang, J. Weng, J. He, E.-P. Lim, H. Yan, and X. Li. Comparing Twitter and traditional media using topic models. In *Proc. 33rd European Conference on IR Research (ECIR)*, volume 6611 of *LNCS*, pages 338–349. Springer, 2011.

[25] Y. Zhong, N. J. Yuan, W. Zhong, F. Zhang, and X. Xie. You are where you go: Inferring demographic attributes from location check-ins. In *Proc. 8th ACM International Conference on Web Search and Data Mining (WSDM)*, pages 295–304. ACM, 2015.