

Running Head: PERSONAL INFORMATION ON TWITTER

Twitter: A Content Analysis of Personal Information

Lee Humphreys, Phillipa Gill, and Balachander Krishnamurthy

*To be submitted for consideration at Information, Communication, & Society.*

Author Note

Lee Humphreys, Ph.D. is an Assistant Professor of Communication at Cornell University. Phillipa Gill, Ph.D. is a Postdoctoral Fellow at the Citizen Lab at the University of Toronto and an Assistant Professor at Stony Brook University. Balachander Krishnamurthy, Ph.D. is lead member of technical staff, research at AT&T Labs--Research.

Funding for this project is provided by the USDA/NIFA, ID 0223492. Special thanks go to Cornell's New Media and Society group for comments on an earlier draft of the paper and to the research assistants who worked on this project: Adam Agata, Ordessia Charron, Madalyn Darnell, Betsy Distelberger, Kim McErlean, Claudia Mei, Elizabeth Newbury, Adi Potashnic, and Deborah Tan.

Please direct all correspondences to Lee Humphreys, Dept. of Communication, Cornell University, 305 Kennedy Hall, Ithaca, NY 14853; [lmh13@cornell.edu](mailto:lmh13@cornell.edu).

## Abstract

Social media provide many opportunities to connect people, but the kinds of personally identifiable information that people share through social media is understudied. This paper presents findings from a content analysis in which we coded the amount and kinds of personally identifiable information of public Twitter messages. Overwhelmingly, public Twitter messages do not include identifiable information such as phone numbers, email, and home addresses. Using Goffman's (1963) concept of "civil inattention", we also coded for whether people articulate the kinds of information that are communicated with others in public space, including locational, temporal, and activity-related information. Our findings suggest that people do share similar kinds of personal information on Twitter that they do in others kinds of physical public spaces, suggesting that people may also be mapping old practices for public social interaction onto networked publics. *(136 words)*

*Key Words:* privacy, social media, Twitter, content analysis, location, civil inattention

### Twitter: A Content Analysis of Personal Information

Information technologies and social media more specifically have complicated traditional notions privacy. boyd and Marwick (2011) argue information was previously private by default, public by effort, however, social media often make information as “public-by-default, private-through-effort” (p.11). This is certainly the case on Twitter, where the default privacy setting is that all messages are public, that is, anyone who signs up for Twitter may see them. All public Twitter messages or “tweets” are also searchable on Twitter, retrievable in Google Search Results (Casey, 2010), and will be archived in the Library of Congress (Raymond, 2010).

Indeed the publicness of Twitter is unlike other popular social networking sites like Facebook and LinkedIn. First, the unidirectional connections are unique on Twitter. Non-reciprocal connections encourage the reading of tweets beyond one’s personal and professional networks (Marwick & boyd, 2011). Furthermore, Bruns & Burgess (2011) argue that the use of hashtags on Twitter can facilitate ad hoc publics to come together around particular topics. Crowd sourcing with tweets (Demirbas, Bayir, Akcora, Yilmaz, & Ferhatosmanoglu, 2010) also reflects the presumed value of the publicness of Twitter. From its inception, Twitter was cross-platform, meaning that users could submit their messages via the web, instant messenger or SMS (“short messaging service” or text message), suggesting that the context for the production and consumption of “tweets” may be further characterized by their publicness. Today 60% of tweets are submitted via a mobile device (McGee, 2012). It might be presumed that many, but certainly not all of those mobile tweets are written and consumed in public spaces.

While research suggests that people have a variety of strategies to manage their publicness and privateness on networked publics (boyd & Marwick, 2011; Marwick & boyd, 2011), there is less evidence examining the specific kinds of private or personal information

people post on social media. Therefore this study seeks to explore the kinds of personal information that people publically share in messages by analyzing the content of a representative sample of public tweets. In doing so, we aim to assess the degree and nature of personally identifiable information shared in Twitter messages and begin to explore the potential implications of sharing certain kinds of personal information in a networked public like Twitter.

### **Social Media and Privacy**

Privacy has been defined as the ability to control what information about oneself and one's group is available to others (Altman, 1976; Westin, 2003). Privacy can be thought of as a dialectical process of managing social interactions and intimacy (Altman, 1976). It is an active process in constant flux depending on contextual and social-psychological needs or desires of an individual. Situating privacy within a relational dialectical frame is appropriate for social media in that all social relations must continually managing their degrees of intimacy and distance (Baxter & Montgomery, 1996). This definition of privacy also highlights the point that it is not just an individual-based concept but can include other social groupings (Bing, 1972). Personal information can have implications for an individual as well as those social and professional relations around him or her.

Extant research has explored the ways people share information about themselves online, and the privacy implications of those disclosures (see Joinson & Paine, 2007 for an overview). Time and again, research has shown that people will disclose more personal information online than they will face-to-face (Joinson & Paine, 2007). Not only do people readily self-disclose in online experimental settings (e.g. Jiang, Bazarova, & Hancock, 2011; Tidwell & Walther, 2002), but they also often disclose personally identifiable information when this is requested by a website (Metzger, 2004). Unlike accounts or profile information, Twitter does not explicitly ask

users to reveal personal information in their tweets. So long as users conform to the 140-character limit, the personal information revealed in Twitter messages is at the complete discretion of users.

While Twitter differs from social network sites like Facebook and MySpace in its format, it can be helpful to look at privacy attitudes and behaviors on these sites in order to better situate this study. A study of the attitudes towards privacy and Facebook use by Acquisti and Gross (2006) found that while privacy concerns predicted Facebook use for older people, it did not predict use for students, suggesting that even when young adults were concerned about privacy issues they were still likely to be active and contributing members of Facebook. Lenhart and Madden (2007) found that as many as two-thirds of teens on social network sites report to have changed their profile settings so that they are not visible to the entire public. In addition, younger teens and females were likely to engage in privacy-protecting behaviors than were older teens and males (Lenart & Madden, 2007). Given that Twitter users have historically tended to be older than Facebook users (Lenhart & Fox, 2009), this may suggest that Twitter users may not engage in as many privacy-protecting behaviors. We see evidence of this in reports about the falling percentage of new Twitter users who change their privacy settings from public to protected when they first join (Moore, 2009), however, this may change as Twitter's average user age decreases (Smith & Brenner, 2012).

boyd and Hargittai (2010) and Stutzman, Capra, and Thomson (2011) argue for the importance of understanding and managing privacy on social media through privacy settings and policies. Default settings can be very powerful in influencing behaviors online. Shah and Kesan (2003) found that people do not change default privacy settings either because they do not know it's possible or they do not have the technological know-how to change their default settings.

These two factors may be increasingly relevant on Twitter as its user base grows and may include less tech-savvy people. In fact, Moore (2009) found in January 2007 that almost 40% of new users to Twitter changed their privacy settings from the default public setting to the protected setting. By August 2009, this number had dropped to less than 8% of new Twitter users changing their privacy settings away from the default (Moore, 2009). Socio-technical expertise and literacy are predictors of changing privacy settings in social media (boyd & Hargittai, 2010).

In addition to literacy and skills, there are norms, which may also influence the use of privacy settings as well. For example, on Twitter there has also been recent backlash against users who have private accounts, suggesting private accounts are “oxymoronic” or “pointless” and that the real value of Twitter is its diverse and open community (e.g. Greenfield, 2012; Neslin, 2011). This suggests that not only are there competing official and unofficial language regarding privacy settings on Twitter, but in addition to needing the socio-technical expertise and literacy, those who wish to use Twitter less publicly may feel social normative pressure to do otherwise.

### **Implications of Sharing**

People use Twitter to share information about themselves as well as to share information publicly available elsewhere on the web, such as breaking news or interesting media such as music, videos, blogs, etc (Mischaud, 2007; Naaman et al., 2010). Honeycutt and Herring (2008) and Naaman et al. (2010) both found that about half of tweets shared information about the author him or herself. However, the dialogic nature of Twitter (boyd, Golder, & Lotan, 2011; Honeycutt & Herring, 2008) suggests the implications of public tweets extend beyond individual users but may directly involve others as well.

Inherent in social media is the dual activity of the production and consumption of social information. Users generate content for other users. Social media reflect the inherent dialectical nature of privacy, as people decide what kinds of personal information to share through these services and what information not to share. There are recent examples of how social media both facilitate and rely on surveillance mechanisms (e.g. Albrechtslund, 2008; Andrejevic, 2007; Humphreys, 2011; Zimmer, 2008). When one cannot control what information about oneself others know, one may also be open to surveillance by others. Lyon defines surveillance as “any collecting or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been gathered,” (2001, p. 2). Social media’s participatory value arises partially from the consumption of others’ social information. When it comes to social media, or all information technology for that matter, one does not know who exactly has access to your personal information or how your information may be used in unintended ways (Alterman, 2003; Nissenbaum, 2004), contributing to what Poster (1990) has called the “superpanopticon”.

Like Bing (1972), Nissenbaum (2004) argues that the context in which personal information is produced has implications for the perception of appropriate access and use. Today many different kinds of information about people can be coupled together to make up a person’s digital or internet footprint. An internet footprint is any information that a person has “created which is online, widely available, and specifically linked to author’s real name” (Garfinkel & Cox, 2009, p. 2). This is an important concept for any study about privacy on Twitter because it suggests that while small bits of communication may in and of themselves provide little to no information about a person’s identity and/or behaviors, in aggregate these

pieces of information together make up an overall footprint of the person that may tell a much deeper, more intimate story.

Additionally, even though people may avoid “real” identification through their online information, such as through online pseudonyms or encryption services, there are an increasing number of technological measures to counter these moves including photo recognition software and computer recovery capabilities (Garfinkel, 2001; Garfinkel & Cox, 2009). Individual messages or bits of information may not seem very incriminating or important, but in a digital age seemingly unrelated data can be retrieved and aggregated with other kinds of information (such as credit card purchases or internet searches from a mobile device) to build a digital footprint.

Even if not aggregated, sharing certain kinds personal information, such as one’s location, may have privacy implications. For example, in June 2009 Israel Hyman, an Arizona-based video podcaster, tweeted that he was looking forward to his family vacation to Saint Louis where they would be visiting family friends for the week. He tweeted again when they had successfully arrived in Missouri. While they were away, their house was broken into, and several thousand-dollars-worth of computer and video equipment were stolen (Van Grove, 2009). According to one news report, Hyman said, "We don't know for sure if that's what caused the break it in, but it sure gives you pause to think about what you're publicly going to broadcast on the internet," ("Man Robbed After Posting His Vacation On Twitter", 2009). This example reminds us that locational information is not always about where one is, but also includes information about where one is not. It can therefore be helpful to look at other forms of public interaction to understand how people might understand the social norms of Twitter as a networked public (Varnelis, 2008).



### **Public Interactions**

There is a rich literature in urban sociology describing public spaces and the social interactions that occur therein (e.g. Gans, 1962; Lofland, 1973; Lofland, 1998). Goffman's (1963, 1971) work in this area is extensive and relevant for a study of public tweets. One of his key insights into urban social interactions is the concept of civil inattention. Goffman (1963) argues that the social norm in public space is to be civilly inattentive to others inhabiting the space. That is, one is aware enough not to bump into others while walking in the park, but one does not typically actively engage others. The old adage: 'it's impolite to stare' suggests that we should not be too attentive to others in public space. It violates the norm of civil inattention.

Civil inattention, however, does not govern all interactions in public. Of course, people of varying degrees of intimacy engage with one another in public space. Goffman (1963) notes that there can be numerous kinds of interactions within the broader interaction set in a public space. Even amongst seeming strangers, the norm of civil inattention can certainly be violated during moments of crisis or breakdown (Goffman, 1963). Indeed Lofland's (1998) work suggests that while civil inattention might be the norm in public space, there are a variety of social interaction and engagements ranging from very short and intense to long-term and casual among people who are relatively unknown to one another in public space.

One can apply Goffman's work on social norms in public space to a networked public like Twitter, such that we can think about potential norms and assumptions that may be at play online. People often map old norms onto new media in public space (e.g. Humphreys, 2005). For example, Hancock, Toma, and Fenner (2008) found that people would often not explicitly articulate that they had seen something on Facebook, but more casually work it into conversation, suggesting that using information about someone from a networked public may

violate certain norms for social interaction outside of the network. Situating tweets within a framework of civil inattention and interactional order has implications for the sharing of personal information online. Whereas one knows that the interactions or tweets are “public” one might assume not only a practical obscurity (Nissenbaum, 2009), but also presume a norm of inattentiveness, that is, others may see information about us in networked publics but they won’t stare or misuse that information.

If we take public space literature as a potential framework for understanding social interactions and privacy norms on Twitter, we can also use it to identify the kinds of personal information we might find on Twitter. For example, one’s physical location is implicitly shared through engagement in offline public spaces. Anecdotes such as the example above of the Twitter user getting robbed suggest that not only do people share their location on Twitter, but that it can have privacy implications. Therefore, this study also asked how often is locational information articulated in public Twitter messages (RQ1).

Another important aspect of public space is that others can see what you are doing. On Twitter people have to explicitly articulate what they are doing. Therefore we also asked how often people share information regarding their activities (RQ2). Unlike in physical public spaces, Twitter users can share about activities that may not be observable in public and may occur elsewhere in their lives. Therefore we also asked the degree to which we can assess where these behaviors are occurring - work, home, outside of work and home (or what one might call public space) (RQ2a). Not only can people reveal current activities, but due to the textual nature of Twitter, they can also reveal information about future or past activities. Therefore we also asked about how often people share information about when activities occur (RQ3).

Public space literature tells us that little information that would be considered personally identifiable (e.g. email, phone number or address) is readily available to others in public and that people are generally only known to one another categorically, that is, based on those characteristics or roles which are directly observable (Bing, 1972; Goffman, 1971). However, to our knowledge no one has examined the kinds of personally identifiable information shared in public tweets. Therefore we also asked how often is personally identifiable information shared in public Twitter messages (RQ4).

## **Methodology**

### **Sampling**

In order to examine the kinds of personal information that was disclosed in Twitter messages, we conducted a content analysis of a sample of public tweets. With Twitter's permission, two of the authors collected an initial sample of users whose tweets appeared in the public timeline. Friends of these users were then crawled using a constrained breadth first search technique. (We maintained a running median,  $m$ , of the number of friends all users had and only collected the first  $m$  friends for each user.) A second set of sample tweets was collected by repeatedly querying the public timeline over three weeks from January 22 to February 12, 2008. Additional details regarding the sampling strategy can be found in Authors (2008). In total, we collected information about 101,069 tweets (message and user ID<sup>i</sup>). From this study, we were also able to attain information about how the tweet had been submitted (e.g. website, text message, Tweetdeck). Because mobile phones are more likely to be used in public spaces, we wanted to see if mobile tweets included systematically different kinds of personal information. We randomly sampled 1050 web and 1050 text message tweets to include in our content

analysis. We coded 1024 web tweets and 1046 text tweets after excluding tweets in a language other than English.

### **Coding Scheme**

We coded each tweets for: 1) personally identifiable information, 2) location information, 3) information regarding the time of day (in addition to the time stamp on all tweets), and 4) who the tweet was about. We also coded for 5) activities and whether these activities could be further sub-coded into 5a) home, 5b) work, or 5c) outside of home and work. The operationalized definition of each coding category and example tweets are given in Table 1.

Tweets were coded as including *personally identifiable information* if they included information that could be directly tied to or associated with an individual, such as email, phone number, or address (Gandy, 1993). While personally identifiable information is directly linked to an individual, it should be noted that Bing (1972) classifies addresses and phone numbers as the least sensitive personal information, as these are often publicly available.

In light of location-aware technologies and privacy concerns (Mills, 2009), we also coded tweets for location information if they included information regarding the *location of people*. Tweets that mentioned locations but did not suggest the location of a person were not coded as having location information. For example, “New York is not for the lighthearted” would not be coded as location of people, whereas “heading to New York City” would be coded as such.

Given the social nature of social media, we also coded tweets for *whom they were about*: the author him or herself, another person/group of people, both self and another, or neither. Sometimes this was indicated with personal pronouns or specific names. Sometimes, however, the author’s role was implied, but not directly stated. Because of the limited characters allowed, it is a convention on Twitter not to use the word “I” but instead just state an activity such as

“eating lunch”. In this case, the message was coded as being about the author him or herself.

Lastly, we coded tweets for *activities*. These include action-related tweets that were related to the activities of the author or their personal network. These tweets are about doing something, about being active. These tweets can be coded regardless of tense. Cognitive activities, such as wanting, thinking, contemplating, hoping, missing, and needing were not coded as activities because they wouldn’t necessarily be observable in physical public spaces.

An activity tweet could be further sub-coded as a specific type of activity: work, home, or outside of home or work. Work tweets involved activities related to work or school, such as homework, reports, interactions with bosses, teachers, or students, etc. Home tweets involved activities that occur in or around the home, such as cooking, cleaning, laundry, gardening, home or vehicle repair, and sleeping. Activities outside of home and work included shopping (unless explicitly mentioned this was done online), going to concerts/theater or eating and drinking out, as well as, running errands, travel (unless explicitly for work), and exercising. Tweets that mentioned media broadly defined as including the internet, computers, books, television and related technology were coded as general activities, unless a location of the activity was specifically mentioned in the tweet.

It is important to note that none of the codes were mutually exclusive. For example, a tweet could be coded as including information about the author and another, work activities and activities outside of home and work, as well as the location of a person.

### **Coding Procedures**

The content analysis involved two pairs and one triad of independent undergraduate coders who were extensively trained on particular categories. Coding teams trained with the first author on specific categories for about four hours per week for between two and a half months to

five months on 628 to 950 messages for each of the eight categories before reliable coding was attained. Reliably coding such short messages proved challenging due to lack of contextual cues; therefore, during these trainings, the codebook was often refined to account for additional insights that emerged during the training process. For example, due to the high number of media-related activities that we came across just while training, we added a media coding category (see Table 1 for definition). If there were urls in the tweet, coders were also instructed to go to the url to help them interpret and code the tweet. Content from the urls was not coded. When coders had reached acceptable levels of reliability (Lombard, Snyder-Duch, & Campanella Bracken, 2002), they coded the random samples of web and text tweets ( $n=2070$ ) from the initial 101,069 public tweets collected. Coders double-coded (or triple-coded, if the coding team was a triad) 24% of this random sample ( $n=499$ ). In order to account for coder drift, the first 300 tweets and the last 199 tweets were double/triple coded. Based on this 24%, Krippendorff's alpha was calculated for each coder category to ensure acceptable levels of inter-coder reliability (Lombard et al., 2002) and ranged from 0.73 to 1.0 (see Table 1). All discrepancies were discussed and consensus coded before the analysis.

## **Results**

Table 2 presents an overall summary of the frequency of privacy-relevant information. Overwhelmingly, public tweets did not include personally identifiable information. Only 0.1% of messages in our sample ( $n = 2$ ) mentioned an email address, phone number or postal address. One of these messages included a personal phone number and the other included an email address, although both included the name of another individual besides the author him or herself. The majority of tweets in the sample were coded as including information about people (77%,  $n = 1576$ ). Most frequently, tweets were about the Twitter user him or herself (self), accounting

for 65.3% of the sample ( $n = 1261$ ), and about 40% of tweets were about another person or group of people. As these were not mutually exclusive categories, almost 25% ( $n = 508$ ) of the tweets involved both the author and another individual or group of people. Only 15% ( $n = 310$ ) of tweets did not mention or imply information about a person or group of people.

Messages that described when user activities occurred (time) accounted for 20.3% of the sample ( $n = 421$ ). Tweets that included information about the location of the Twitter user were less prevalent: 12% of tweets mentioned the location of a person ( $n=249$ ). Most frequently (82%,  $n = 204$ ) location tweets were about the author him/herself ( $\chi^2 = 32.33$ ,  $df = 1$ ,  $p < .001$ ). Only 3% ( $n = 62$ ) of the sample included both location and time and were about the author him/herself.

Overall, activities accounted for 41% ( $n = 852$ ) of our sample. We were only able to further sub-code 61% ( $n = 521$ ) of the activities into home activities, work activities, or activities outside of home a work. Of the sub-coded activities the most frequent was outside of home and work ( $n = 310$ ), which was more likely to be sent via text message than through the website,  $\chi^2(1, n = 310) = 79.454$ ,  $p < .001$ . Home and work activities were more likely to be submitted via the web, respectively  $\chi^2(1, n = 108) = 9.479$ ,  $p < .01$  and  $\chi^2(1, n = 128) = 6.235$ ,  $p < .05$ . Of the 331 activity tweets not further sub-coded into home, work, or outside of home and work, 69% ( $n = 229$ ) of them were coded as media-related.

Activities were also likely to include information regarding the person's location and include the time of the activity, respectively  $\chi^2(1, n = 167) = 78.453$ ,  $p < .01$  and  $\chi^2(1, n = 239) = 53.174$ ,  $p < .01$ . This was largely driven by activities outside of home and work, where these activities were largely locationally defined,  $\chi^2(1, n = 129) = 301.552$ ,  $p < .01$ . For example,

people would often tweet they were at a particular restaurant or store rather than they were eating out or shopping.

### **Discussion**

Messages confined to 140 characters may seem and even may be innocuous, but they can still include personal information. Overwhelmingly, tweets in our sample were about people, and most often about the Twitter user him or herself. That said, 40% of sampled tweets were about other people besides the Twitter user. This suggests that as people share personal information on Twitter, they aren't just sharing their own information; rather, they share information concerning other people as well. This is an important difference from social interaction in physical public spaces where people most often communicate their own personal information (Goffman, 1963).

Our study suggests that Twitter users almost never share personally identifiable information on the service. People may know to be careful about sharing phone numbers, home addresses and email addresses publicly; however, people may be sharing enough bits of information that combined with ambient information, such as usernames and locations, could lead to identity and personally identifiable information.

Additionally, a second tier of personally identifiable information may raise concerns about who has access to information about where and when people are. About 20% of tweets indicated when people engage in activities and about 12% indicated where they were or will be. While this suggests that people do not usually indicate when and where they are or will be, amid the flood of 400 million tweets per day (Farber, 2012), this number may translate to as many as 48 million tweets per day where an author shares information about his or her location with the public.



One of the important points about location information is that when people say where they are or where they will be, it also indicates where they are not. One does not have to explicitly say one's home will be vacant while on vacation. It's not always about where a person is, but where they are not that raises concern. Additionally, with the incorporation of Twitter's GeoAPI, which automatically attaches geo-location to tweets and automatically time stamps them, users no longer need to explicitly articulate a time and location to share this type of information when using the service (Elwood & Leszczynski, 2011). Additionally, users can link their Foursquare check-ins to Twitter. Together these might suggest our findings regarding the frequency of location sharing on Twitter are lower than in practice. Despite the time stamp, users' temporal articulation within tweets has important implications for privacy because it suggests both future and past activities, which can raise additional privacy concerns.

While we may share locational and temporal information with strangers every time we physically venture out into public space, the important difference between sharing temporal and locational information through a networked public like Twitter and implicitly sharing it with those inhabiting the public space with us is the ease with which that information can be coupled with other kinds of digital information (Garfinkel, 2001). Privacy concerns that arise from robbery or stalking are among the most egregious violations of civil inattention, but they are the exception not the rule.

Temporal and locational information disclosures do not always lead to dire consequences. Sometimes people say they're at one place when they are actually at another (e.g. calling in sick, but going out). Social awkwardness and embarrassment can arise when people use social media to communicate their actual locations, whether it be through tweets or check-ins, that place people in certain locations at certain times when they should be elsewhere (Lindqvist, Cranshaw,

Wiese, Hong, & Zimmerman, 2011). We know that people often engage in white lies to avoid socially awkward situations with mobile devices (Birnholtz, Guillory, Hancock, & Bazarova, 2010). Twitter provides another way to broadcast oneself to a variety of audiences, potentially increasing the number of opportunities for people to get caught in their white lies. However, the norm of civil inattention might suggest that while people may notice such white lies within the networked public, they may not necessarily act on it.

### **Study Limitations**

There are several limitations to this study. First, content analyses such as this can never shed light on motivations, understandings, or intentions surrounding that content. We thus cannot make any claims about how Twitter users think about privacy, personal information or civil inattention on Twitter. However, this is the first content analysis, to our knowledge, that does not rely on hashtags or keyword sampling but a random sample of tweets that also report reliability measures regarding the content on Twitter which is an important contribution of the study. However, we were only able to conduct a random sample of tweets because the data collected for this sample was from 2008 when the number of tweets generated per day was significantly smaller. Twitter has grown tremendously since then (Farber, 2012). Therefore we do not know if the trends regarding personal information in the public tweets in 2008 documented here are similar or different than trends we would see currently on Twitter. On the one hand, early adopters can help to establish norms of usage (Rogers, 1983). On the other hand, early adopter usage does not always mirror that of later adopters (Preece, 2004), and future work should assess trends in tweet content and their implications for privacy and surveillance. Additionally, while our tweets were primarily written from the perspective of a singular person, organizations and groups have flocked to Twitter as a means of connecting with customers and

constituents. Thus what it meant to tweet a phone number or email address has likely changed since 2008 given that it may not be personally identifiable. We also only analyzed public tweets and not private tweets or direct messages. In particular, it would be interesting to compare the content of direct messages by users with public accounts and their public tweets.

Another potential limitation is that our unit of analysis was an individual public tweet. We did not couple tweets by the same user, nor did we couple these with profile information. Reading tweets over time from the same person could expose many more habitual practices regarding location and time than just one individual tweet could reveal. Similarly, information in tweets may take on greater significance when coupled with a Twitter user's profile information, which includes a person's user- "name", "location", and "bio". In addition to one's universe of tweets and profile information, a single tweet can also easily be coupled with other information online to allow for much greater privacy concerns than any individual message alone (Gandy, 1993).

### **Directions for Future Work**

Sharing personally identifiable information through social media is not necessarily problematic. It is important to keep in mind that information-sharing through social media is a dialectical process (Altman, 1976). We see sharing of personal information on Twitter because there are benefits that come from sharing personal information in social and public ways (Hampton & Wellman, 1999). However, the dialectical framework suggests that the act of sharing calls to light the act of not sharing - what is tweeted compared to what is not tweeted. This study was one of the first to reliably code what was tweeted but future research should examine what kinds of things people avoid tweeting about. Research suggests that active Twitter users do avoid certain topics in order to navigate multiple audiences (e.g. personal and

professional relations) (Marwick & boyd, 2011). Comparison between public and private accounts would also allow us to better understand the role of perceived audience and control over one's information may have on what kinds of things get tweeted and what does not.

Today's social media environment is best characterized as "public-by-default, private-through-effort" (boyd & Marwick, 2011, p. 11). While various kinds of personal information may be publicly available through social media like Twitter, Nissenbaum (2009) argues that its availability is not necessarily problematic from a privacy perspective, but its inappropriate use is. When information is created in one context and used in a dramatically different context, it causes privacy concerns. Goffman's (1963) concept of civil inattention may be an important way for understanding how people can actively engage with social media while acknowledging the dialectical nature of such social interactions. While they are publicly available for others to see, the appropriate or civil way to engage with others' information in this way is to perform inattention. Civil inattention allows us to interact with others in networked publics like Twitter without potentially violating privacy. The performativity of civil inattention also resonates with Papacharissi (2012) recent finding that performance is quite central to Twitter use. Rather than suggest people not engage in public forms of communication through social media or that they create private accounts that may not facilitate the same kinds of information exchanges as public ones, civil inattention allows us to interact in public while maintaining a sense of privacy.

While Goffman (1963) suggested civil inattention was a social norm, one can see design features within Twitter itself that afford civil inattention. For example, the difficulty in accessing older tweets of users reflects a civil inattentiveness that the Facebook timeline does not. Future research might more closely examine how technological affordances and social norms reflect civil inattention as a means of managing the dialectical processes of engaging in and through

social media. As social media continue to proliferate, privacy-shaping behaviors and conventions are likely to shift. Now is a critical time to examine and, in turn, shape these social and technological conventions.

### References

- Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the facebook*. Paper presented at the 6th International Workshop on Privacy Enhancing Technologies, June, Cambridge, UK.
- Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, 13(3). Retrieved from <http://firstmonday.org>
- Alterman, A. (2003). "A piece of yourself": Ethical issues in biometric identification. *Ethics and Information Technology*, 5(3), 139-150.
- Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, 8, 7-29.
- Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, KS: University Press of Kansas.
- Baxter, L. A., & Montgomery, B. M. (1996). *Relating: Dialogues and dialectics*. New York, NY: Guilford Press.
- Bing, J. (1972). Classification of personal information, with respect to the sensitivity aspect. *Proceedings of the First International Oslo Symposium on Data Banks and Society*, Universitetsforlaget, Oslo, 178-192.
- Birnholtz, J., Guillory, J., Hancock, J. T., & Bazarova, N. (2010). "on my way": Deceptive texting and interpersonal awareness narratives. *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work, Savannah, Georgia*, 1-4. doi:10.1145/1718918.1718920.
- boyd, d., Golder, S., & Lotan, G. (2010, January). *Tweet, tweet, retweet: Conversational aspects of retweeting on Twitter*. Paper presented at the Forty-Third Hawaii International Conference on System Sciences (HICSS-43), Koloa, Kauai, Hawaii.

- boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8), <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>.
- boyd, d., & Marwick, A. E. (2011). *Social privacy in networked publics: Teens' attitudes, practices, and strategies*. Paper presented at the Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", September 22. Oxford, UK.
- Bruns, Axel & Burgess, Jean E. (2011) The use of Twitter hashtags in the formation of ad hoc publics. In *6th European Consortium for Political Research General Conference, 25 - 27 August 2011*, University of Iceland, Reykjavik.
- Casey, D. (2010). Replay it: Google search across the Twitter archive. *The Official Google Blog*. Retrieved from <http://googleblog.blogspot.com/2010/04/replay-it-google-search-across-twitter.html>
- Demirbas, M., Bayir, M. A., Akcora, C. G., Yilmaz, Y. S., & Ferhatosmanoglu, H. (2010). Crowd-sourced sensing and collaboration using twitter. *Proceedings of the 2010 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, Canada*, 1-9. Retrieved from <http://www.cse.buffalo.edu/~mbayir/papers/crowdsource.pdf>
- Elwood, S., & Leszczynski, A. (2011). Privacy, reconsidered: New representations, data practices, and the geoweb. *Geoforum*, 42(1), 6-15.
- Farber, D. (2012). Twitter hits 400 million tweets per day, mostly mobile. Retrieved from [http://news.cnet.com/8301-1023\\_3-57448388-93/twitter-hits-400-million-tweets-per-day-mostly-mobile/](http://news.cnet.com/8301-1023_3-57448388-93/twitter-hits-400-million-tweets-per-day-mostly-mobile/)

- Gandy Jr., O. H. (1993). *The panoptic sort: A political economy of personal information*.  
Boulder, CO: Westview Press.
- Garfinkel, S. (2001). *Database nation: Death of privacy in the 21st century*. Sebastopol, CA:  
O'Reilly & Associates, Inc.
- Garfinkel, S., & Cox, D. (2009, February). Finding and archiving the internet footprint. Paper  
presented at First Digital Lives Research Conference: Personal Digital Archives for the  
21st Century, London, England.
- Gans, H. (1962). *The Urban Villagers*. New York: The Free Press of Glencoe.
- Goffman, E. (1963). *Behaviors in Public Places: Notes on the social organization of gatherings*.  
New York: Free Press.
- Goffman, E. (1971). *Relations in Public: microstudies of the public order*. New York: Harper &  
Row.
- Greenfield, J. (2012, April 27). How to use Twitter: Live chat recap. from  
[http://www.chicagonow.com/greenfields-village/2012/04/how-to-use-twitter-live-chat-  
recap/](http://www.chicagonow.com/greenfields-village/2012/04/how-to-use-twitter-live-chat-recap/)
- Hampton, K., & Wellman, B. (1999). Netville online and offline: Observing and surveying a  
wired suburb. *American Behavioral Scientist*, 43(3), 475-492.
- Hancock, J. T., Toma, C., & Fenner, K. (2008). I know something you don't: Use of asymmetric  
personal information for interpersonal advantage. *Proceedings of the ACM conference on  
Computer-Supported Cooperative Work (CSCW 2008)*, San Diego, CA.
- Honeycutt, C., & Herring, S. (2009). Beyond microblogging: Conversation and collaboration via  
Twitter. *Proceedings from the Forty-Second Hawai'i International Conference on  
System Sciences (HICSS-42), USA*, 1-10.



- Humphreys, L. (2005). Social topography in a wireless era: The negotiation of public and private space. *Journal Technical Writing and Communication*, 35(4), 367-384.
- Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication*, 61, 575-595.
- Jiang, L., Bazarova, N., & Hancock, J. T. (2011). From perception to behavior: Disclosure reciprocity in computer-mediated and face-to-face interactions. *Communication Research*. Doi: 0.1177/0093650211405313.
- Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy & the Internet. In K. M. Adam, N. Joinson, & T. Postmes (Eds.), *The Oxford handbook of Internet psychology* (pp. 237-252). New York: Oxford University Press.
- Lenhart, A., & Fox, S. (2009). *Twitter and status updating*. Washington DC: Pew Internet and American Life.
- Lenhart, A., & Madden, M. (2007). *Teens, privacy & online social networks*. Washington DC: Pew Internet and American Life Project.
- Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., & Zimmerman, J. (2011). *I'm the mayor of my house: examining why people use foursquare - a social-driven location sharing application*. *Proceedings of the 2011 annual conference on Human Factors in Computing Systems (CHI2011)*, 2409-2418.
- Lofland, L. (1973). *A world of strangers: Order and action in urban public space*. New York: Basic Books.
- Lofland, L. H. (1998). *The public realm: Exploring the city's quintessential social territory*. New York: Aldine De Gruyter.

- Lombard, M., Snyder-Duch, J., & Campanella Bracken, C. (2002). Content analysis in mass communication: Assessment and reporting of intercoder reliability. *Human Communication Research, 28*(4), 587-604.
- Lyon, D. (2001). *Surveillance society: Monitoring in everyday life*. Buckingham: Open University Press.
- Man Robbed After Posting His Vacation On Twitter. (2009). Retrieved from <http://www.wpxi.com/news/19648421/detail.html>
- Marwick, A. & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1): 114-133.
- McGee, M. (2012, June 8). Twitter: 60% percent of users access via mobile. Retrieved from <http://marketingland.com/twitter-60-percent-of-users-access-via-mobile-13626>.
- Metzger, M. (2004) Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer Mediated Communication, 9*(4), 335-361. doi:10.1111/j.1083-6101.2007.00328.x
- Mills, E. (2009, June 8). Twitter user says vacation tweets led to burglary. Retrieved from [http://news.cnet.com/8301-1009\\_3-10260183-83.html](http://news.cnet.com/8301-1009_3-10260183-83.html)
- Mischaud, E. (2007). *Twitter: Expressions of the whole self* (Unpublished master's thesis). London School of Economics, London, UK.
- Moore, R. J. (2009, October 5). Twitter data analysis: An investor's perspective. Retrieved from <http://www.techcrunch.com/2009/10/05/twitter-data-analysis-an-investors-perspective/>
- Naaman, M., Boase, J., & Lai, C.H. (2010). Is it really about me? Message content in social awareness streams. *Proceedings of the ACM Conference on Computer Supported Collaborative Work (CSCW2010), USA*, 189-192.

- Neslin, L. (2011, October 24). Hashtag humor: Private Twitter accounts are oxymoronic from <http://www.qchronicle.com/2011/10/hashtag-humor-private-twitter-accounts-are-oxymoronic/>
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, 101-139.
- Nissenbaum, H. (2009). *Privacy in context*. Stanford, CA: Stanford Law Books.
- Papacharissi, Z. (2012). Without You, I'm Nothing: Performances of Self on Twitter. *International Journal of Communication*, 6, 1989-2006.
- Poster, M. (1990). *The mode of information: Poststructuralism and social construct*. Chicago, IL: University of Chicago Press.
- Preece, J. (2004). Etiquette online: From nice to necessary. *Communications of the ACM*, 47(4), 56-61.
- Raymond, M. (2010). How tweet it is!: Library acquires entire Twitter archive, *Library of Congress Blog*. Washington D.C.: Library of Congress. Retrieved from: <http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/>
- Rogers, E. (1995). *Diffusion of Innovations* (4th Edition ed.). New York: The Free Press.
- Shah, R., & Kesan, J. P. (2003). Manipulating the governance characteristics of code. *Info* 5(4), 3-9.
- Smith, A., & Brenner, J. (2012). *Twitter Use 2012*. Washington D.C.: Pew Internet and American Life Project.
- Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27(1), 590-598.
- Tidwell, L. C., & Walther, J. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time.

*Human Communication Research*, 28(3), 317-348.

Van Grove, E. (2009). Twitter your way to getting robbed. Retrieved from

<http://mashable.com/2009/06/01/twitter-related-burglary/>

Varnelis, K. (Ed.). (2008). *Networked publics*. Cambridge, Mass.: MIT Press.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453.

Zimmer, M. (2008). The externalities of search 2.0: The emerging privacy threats when the drive for the perfect search engine meets Web 2.0. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/>.

Table 1

*Coding Categories*

Category	Definition	Example	Intercoder Reliability <sup>a</sup>
Personally identifiable information	Information that could be directly tied to or associated with an individual such as email, phone number, or address	“is looking for a StarCraft key...anyone? [omitted]@gmail.com please and thank you so much, now I can play against my son.”	1.00
Location	Information regarding the specific location of people, i.e.: country, state/territory (e.g. east coast), city, and specific locales	“I'm back in the states...bout to get off the plane and go clear customs and immigration”	.74
Time	Information about when activities occur or references to <i>specific</i> time such as today, tomorrow, tonight, morning, now, [specific time or date]	“Prep for a long ride tomorrow. Saddle height up and patsa [sic] for dinner. And we went to the pub. Oops!”	.80
About whom (self, other person/ people, both)	Person [people] who is being discussed in the message, the person doing the activity of the tweet or the person to whom an activity is being done. A single Twitter message can involve multiple people. Must be a human being, alive or dead.	“at sears buying another 30 lbs dumbbell” “oh yeah, sat next to elvis costello at my local sushi bar”	.89
Activities	Action-related tweets, related to the activities of the author or their personal network. These tweets are about doing something, about being active.	“Just updated my blog”	.79
Home Activities	Activities occurring at or around the home.	“Making lasagna for dinner.”	.73
Work Activities	Activities occurring at or related to work or school.	“Finished the report for my boss.”	.78
Outside of Home & Work Activities	Activities occurring in public or semi-public spaces or travel/transit.	“Running errands at the mall.”	.80
Media	Mention of media, internet, or communication technology (urls not included)	“Just watched American Idol”	.81

Table 2  
*Overall Frequency of Categories*

Category	Frequency
Personally identifiable information	0.1% ( <i>n</i> =2)
Location	12.0% ( <i>n</i> =249)
Time	20.3% ( <i>n</i> =421)
Self	66.4% ( <i>n</i> =1375)
Other	39.8% ( <i>n</i> =823)
Both Self & Other	24.5% ( <i>n</i> =508)
Activities	41% ( <i>n</i> =848)
Work activities	6% ( <i>n</i> =124)
Home activities	5% ( <i>n</i> =103)
Outside of home and work activities	15% ( <i>n</i> =310)
Media	35% ( <i>n</i> =724)
Total Tweets coded	2070

<sup>i</sup> User ID is different from names or usernames. We specifically wanted to not collect the name to maintain some privacy of the tweets.