Privacy Leakage in Mobile Online Social Networks

Balachander Krishnamurthy
AT&T Labs – Research
Florham Park, NJ USA
bala@research.att.com

Craig E. Wills
Worcester Polytechnic Institute
Worcester, MA USA
cew@cs.wpi.edu

Abstract

Mobile Online Social Networks (mOSNs) have recently grown in popularity. With the ubiquitous use of mobile devices and a rapid shift of technology and access to OSNs, it is important to examine the impact of mobile OSNs from a privacy standpoint. We present a taxonomy of ways to study privacy leakage and report on the current status of known leakages. We find that all mOSNs in our study exhibit some leakage of private information to third parties. Novel concerns include combination of new features unique to mobile access with the leakage in OSNs that we had examined earlier.

1 Introduction

The growth in Online Social Networks (OSNs) continues unabated with around 10% of the world's population currently on one of hundreds of OSNs. A handful are extremely popular with hundreds of millions of users. Separately there has been an explosion of popularity of mobile devices with nearly 3 billion users (nearly half of the world's population) who have cell phones. Increasingly, mobile devices have become smarter: they go well beyond voice communication and play music and videos, access the Internet over WiFi and their own communication networks. Not surprisingly, an increasing fraction of accesses to OSNs are now via mobile devices.

Correspondingly there has been a growth in new *mobile* OSNs (mOSNs) that primarily cater to 'mobile' users, who access them largely via mobile devices. Such convergence is due to the natural movement from the connections over telephone between friends to linkage over OSNs. Mobile devices provide ubiquitous access to the Web. Many existing OSNs have created content and access mechanisms tailored to mobile users to account for the limited bandwidth, latency, and screen sizes of the devices. A recent survey showed that nearly a quarter of mobile users in UK visited an OSN via mobile devices [9]. Backing this survey up, Facebook, the OSN with the largest number of users recently announced [2] that a quarter of their users visit their OSN site via a mobile device every month. Another survey reported that traffic on the mobile Web doubled in 2009 [11].

All of these factors have resulted in a dramatic growth in traffic to mobile OSNs and parts of traditional OSNs with content tailored for mobile devices. A traditional Web site for access from desk/laptop continues to be important for mOSNs. Access to mobile OSNs comes in different forms including mobile-specific interfaces and content. There has been a tremendous growth in "apps" (applications) for mobile devices and many are available for customized interaction with mOSNs. Some OSNs, most notably Facebook and Twitter, provide APIs for connections to their site. These programmatic interfaces were not designed specifically for mobile devices but they are used by mOSNs to share the activities of a mOSN user with other OSNs.

Earlier [6, 7] we characterized privacy in OSNs and highlighted various vectors of privacy leakage in popular OSNs. Here, we examine privacy leakage in interactions with mobile OSNs and include some special-purpose social networks (such as Flickr, Yelp) that we did not study earlier. We examine two different kinds of mOSNs in our work: popular OSNs such as Facebook and MySpace that have evolved to allow access from mobile devices, as well as the new mOSNs, such as Foursquare and Loopt, designed specifically to be accessed by mobile devices. There is evidence that Facebook and MySpace have received most of the accesses from mobile devices [12] with growth in mobile access to Twitter as well.

In our work, we enumerate privacy issues that are new in mobile OSNs. These typically arise due to new features that are first order in mobile OSNs. For example, the contextual information of a user, expressed in the form of presence on a mOSN and geographical location is a feature that is widespread in the mobile environment. The ability to factor in the user's location allows

more tailoring than is possible through access via wired and WiFi networks [8]. Location has been described as the missing link between the real world and OSNs [13].

As we expect mobile access to become widespread on traditional OSNs, we should examine ways by which the new features interact with existing privacy issues. We explore the interesting issue of *combination leakage*: are there pieces of information that are on traditional OSNs that when combined with new features in mobile OSNs result in privacy leakage? Also, we need to see if existing privacy protection measures are obsoleted as a result of interaction with the new environment.

The use of mobile OSNs is relatively new and we examine privacy issues in using them. However, we stress that our work is not about examining all mobile accesses such as using a cell phone to access a bank account which may also involve leakage of private information. One reason to examine general mobile privacy is that user's may carry over notions of expected privacy from the use of mobile devices to any new applications such as mOSNs. European regulators have warned of higher privacy losses as a result of searching the Internet via cellphones [4]. The primary additional private information being lost was user's location information. A study examining privacy and security done in 2008 also warned about leakage of temporal and geographical information in the mobile context [3].

The rest of the paper is organized as follows: Section 2 examines the various interfaces for interacting with mOSNs along with the external interactions emanating from mOSNs. Section 3 enumerates the taxonomy of privacy issues in mobile OSNs and our reasons for studying them. Section 4 presents our detailed study of mOSNs with the results appearing in Section 5. We summarize our results with a look at future work in Section 6.

2 Interfaces and Interconnections

The growth of mOSNs has been fueled by the desire to bring social networking to mobile devices while retaining access to traditional social networking sites. This growth has been two pronged: traditional OSNs have created mobile Web sites and mobile applications for users to access their OSN account while new mobile OSNs have been created to explicitly take advantage of mobile device features such as the capability to obtain precise current location. The resulting landscape has been a melding of new and old where each mOSN provides a variety of interfaces for access. Newer mOSNs ease the transition by taking advantage of API connection features of traditional OSNs to present an integrated social networking experience for users. These ideas of multiple interfaces and interconnections between users are captured in Figure 1, along with third-party servers that aggregate information for advertising and analytics.

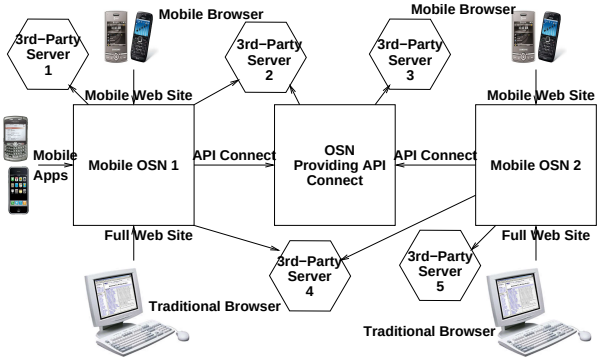

Figure 1: Interfaces and Interconnections for mOSNs

Figure 1 shows that mOSNs may have up to four types of interfaces, which are simply portals to the content of the mOSNs. First, a mOSN must minimally support a mobile Web site serving content adapted to the constraints of a mobile device browser. Second, it may support a traditional (full) Web site accessible via a traditional browser as a matter of convenience for the desktop user and to simplify the upload of (often, large) content. Third, it may support access via mOSN-specific applications created specifically for a device using a well-defined API. The API allows the mOSN user interface to be customized for the device. Device-specific mobile applications need not access the same server as the mobile Web site. Finally, it may allow connections with an OSN that provides an API Connect feature (e.g. Facebook and Twitter) for sharing content, such as updates with the OSN. Figure 1 shows two mOSNs, each with a mobile and full Web site interface as well as an interconnection with an OSN supporting a Connect API. In addition, applications on different devices exist for mOSN1.

Note the distinction between a device and an interface. A device such as a smart phone could be used to access the mobile or full web site via a mobile browser as well as a device-specific application tailored for a mOSN. A desktop user would likely use a traditional browser to access the full Web site, but could modify the User-Agent field in their browser to access the mobile site.

Figure 1 also shows the existence of third-party servers. These third-party servers may obtain information from both mobile and traditional OSNs, such as 3rd-party Server 2 in the figure. Some third-party servers, such as 3rd-party Server 4, may concentrate on the mobile market. From a privacy leakage standpoint, the connection service creates problematic scenarios. For example, a user's location shared with mOSN1 via the user's smart phone may be leaked to 3rd-party Server 3, which has no immediate direct relationship with mOSN1.

3 Taxonomy of Privacy Issues

We consider two classes of mobile OSNs: 1) traditional OSNs (such as Facebook and MySpace) that have expanded to embrace access via mobile devices; and 2) applications and OSNs that were created largely to deal with the new mobile context. The latter class forms a majority in our study. Our taxonomy may differ between the two classes. Privacy issues that were a concern in traditional OSNs, such as permissive sharing of personal information to all OSN users as well as leakage of private information to third-parties, remain relevant to the former class while they need to be examined anew for the latter class. The manner of examination of privacy issues takes into account the different interfaces and interconnections outlined in the previous section.

In addition to privacy issues observed for traditional OSNs, which may be exacerbated as a result of the new features in mOSN, we examine privacy issues that are new in the mobile context and ones that result from interaction between traditional OSNs and mOSNs. The concepts that are either novel or play a predominant role in mOSNs include *presence* and *location*, which we explain in more depth below. These concepts have played a lesser role in traditional OSNs, although determining a user's presence has become more important in an OSN such as Facebook that seeks to provide an instant messaging service to its users. Twitter has recently allowed users to add their location information even when users access their traditional site.

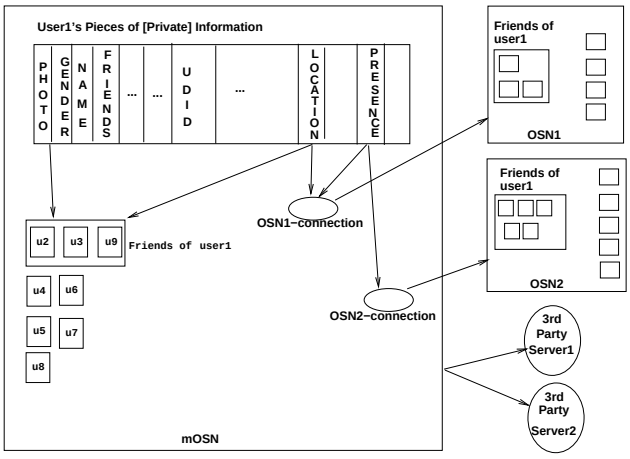

Figure 2: Potential Privacy Leakage vectors in mOSNs

Figure 2 lists a few of the mOSN user's pieces of private information and some of the entities (both inside and outside the mOSN) to which information might leak. We explore privacy leakage along two tracks: the personal information that may be sent and the destination to which it could be sent. The latter is important in the context of mOSNs because there are a larger set of possible destinations due to the expanded features in mOSNs. There are at least three possible destinations: internally within the mOSN (e.g., to a user's friends, networks/communities, or everyone), externally to other traditional OSNs through the connection feature (and thus to the user's contacts in those traditional OSNs which can be limited to their friends or accessible to everyone), and finally to third-party aggregators and advertisers.

Many mOSNs *do* provide a range of privacy settings. However, the multi-dimensional nature of the issue makes the problem of protecting information significantly harder. Consider for example the amount of information a user has to keep track of in interacting with a mOSN. They have to be aware of the duration of any privacy setting they have made. When they allow some information, such as location, to be used by the mOSN for a legitimate purpose (locating them on a map, say), they have to be aware that it might be handed over to third-parties. They have to keep track of what subset of users have access to which subset of their private information: their friends, their friends who are currently online on this mOSN, their friends in other mOSNs, etc. Additionally, popular atomic actions on mOSNs such as 'checking in' at a location reveals much about the user: their presence, their location, and the current timestamp. The richer the features of a mOSN, the more complex the results of a single action would be.

As to what personal information is sent to different places, there is considerable variance. User's presence, location, etc. can be made known to other users on the mOSN, passed on to the external OSNs and the third parties. Contents of updates are typically available to the local mOSN and external traditional OSNs.

Presence on an OSN is not a new concept, but in most traditional OSNs users were not automatically made aware of the presence of their friends (or any other users). Such a feature has been long available in instant messaging systems. Many mOSNs, on the other hand, allow users to indicate their presence via a "check-in" mechanism, where a user establishes their location at a particular time. Presence is an important notion in mOSNs as one of their key features is the notion of checking physical co-location of users. Users who are not present on a mOSN are not likely to participate in any dynamic interactions. The indication of presence allows their friends to expect quick response. Sharing presence more broadly than just with friends allows meeting new people who are members of the same mOSN.

A user's availability to communicate is indicated by presence and the notion of presence exists independent of a closely related notion: that of location. Location is a widely used feature in mOSNs and until recently was

not even an availablefeature in traditional OSNs. The ubiquity of GPS and the ability to automatically locate oneself, has led to location being considered a basic feature of many mOSNs. In our study, a number of the mOSNs have limited functionality if users do not disclose their location. With such a definition, location might be viewed as essential for the proper functioning of a mOSN and thus not a crucial concept from the purview of privacy. However, users may not want to disclose their location beyond their set of friends to avoid potential pitfalls of preying users [10]. Many mOSNs allow such disclosure to be limited to friends or to friends that are within a given distance from the user. It is important to be aware that users can indicate their presence on an mOSN without disclosing their exact location.

There are additional pieces of privacy that are at risk of leakage in mOSNs—these include information related to the mobile device. For example, mobile devices typically have a unique device identifier for various purposes, such as installing approved applications on the specific user's mobile device. This is a common identifier present in all mobile devices. For example, on the Apple iPhone it is a string called UDID[1], on the Android it is Android ID[2] and on the Windows Phone it is the DeviceUniqueId, which consists of a platform ID (identifying the type of hardware device) and a preset ID (identifying the specific device) and is of varying length[3].

There is a potential privacy issue if this unique identifier is leaked to a third-party via an application, which has access to the identifier through the device's API. If leaked, this identifier could be associated with a user's identity and be used to track an unknowing user's actions across different applications.

Perhaps the most interesting issue that raises significant new privacy concerns is the interaction potential between mOSNs and traditional OSNs. Such an interaction has already been made available in many mOSNs to increase their popularity. Mobile OSNs encourage users to link their activities on mOSNs with traditional OSNs like Facebook and Twitter. Such connections are useful to users who, while interacting with a mOSN can expect some of their actions to show up on traditional OSNs and be visible to their friends there. The information supplied by users and the degree of interconnection based on API connections varies across mOSNs. For example, if a user discloses location to a mOSN and is automatically connected to Facebook or Twitter, then friends on those OSNs may also be able to see this information. However the location information is posted on the user's Facebook wall or Twitter timeline and available by default to all users in each OSN.

[1] http://developer.apple.com/iphone/library/documentation/UIKit/Reference/UIDevice_Class/Reference/UIDevice.html

[2] http://developer.android.com/reference/android/provider/Settings.Secure.html

[3] http://blogs.msdn.com/jehance/archive/2004/07/12/181116.aspx

4 Study

Given the number of potential privacy issues discussed in the previous section, we designed a study to determine which of these problems occur in current mOSNs and to what extent. The study was carried out in three parts: 1) identifying an appropriate set of mOSNs for study; 2) enumerating a specific set of research issues to examine for each; and 3) establishing a methodology to use in studying these issues for each mOSN.

4.1 Mobile OSNs for Study

Although the world of mobile OSNs is relatively new, there have been several dozen that have started within the last few years. Most of them are startup companies that have attempted to latch on to the popularity of mobile devices and take advantage of the low barrier for entry. A cursory examination of available mOSNs generated over 75 candidates. Normally, one would apply standard filtering criteria of popularity, feature richness, etc. to identify a reasonable subset to study. However, given the novelty of the field we decided not to eliminate mOSNs just because they are not yet well known.

We used the following criteria of inclusion (and exclusion) of candidate mOSNs for our study.

Account: The candidate mOSN must require users to establish an account associated with an email address, a cell phone number, or both. This necessary condition allowed us to filter out ones that may be transient.

Social aspect: The candidate mOSN must support social interactions with friends within the site. This criterion excluded sites that are simply aimed at integrating mobile users with regular accesses to their site.

Mobile access: The candidate mOSN must provide at least one interface that tailors the content for one or more mobile devices. A popular OSN that allowed access to their traditional Web site with no provisions made for the different requirements of mobile devices and mobile access would not qualify. New challenges arise in tailoring the content and both restricts and diversifies the set of features in an OSN.

Many mOSNs necessarily make use of location and some of them have also developed mobile device-specific applications. However we did not deem these to be a necessary condition for inclusion. We believe that the availability of location information in many mobile devices will quickly lead to use of that information by any mOSN that currently lacks this feature. Device-specific applications improve access to the mOSN on the given device, but are not a requirement for inclusion.

As a secondary criterion we filtered the candidate mOSNs meeting the necessary conditions listed against popularity metrics available from Quantcast and Alexa. We thus established a study set of 20 mOSNs, 7 of which are traditional OSNs that were part of our earlier study [7]—Bebo, Facebook, Hi5, Linkedin, Livejournal, MySpace and Twitter. We added two special purpose social networks Flickr and Yelp; the rest 11 were not in existence prior to the widespread use of mobile devices—Brightkite, Buzzd, Dopplr, Foursquare, Gowalla, Gypsii, Loopt, Radar, Urbanspoon, Wattpad and Whrrl.

While the availability of device-specific applications was not a criterion for selection, we wanted to study this interface for mOSNs that provided it and thus we examined mOSNs with applications for various devices. We did so based on information provided on the mobile and full Web site of each mOSN and by consulting device-specific lists of social networking applications. We found that 19 (all but Hi5) of our mOSNs had applications for the Apple iPhone. Currently, ten have applications for the Blackberry, six each for the Google Android and the Palm, and three for the Windows phone from Microsoft.

After our study set was chosen, the pre-manufactured social network Buzz was introduced with users organized into friendship networks based upon their set of frequent correspondents in the email service called Gmail. Avoidable privacy breaches in the initial version included the default of making the list of contacts public on a user's profile, automatic linkage to other internal services (photo albums and news reader feeds), information about people who never joined being exposed as a result of being a frequent correspondent with a participant, etc.—primarily due to designers' default choice of opt-out instead of opt-in. Following widespread criticism, all of these issues were fixed shortly after the initial release. Since our study is about the more organically grown mOSNs, we did not study Buzz.

4.2 Research Issues

The taxonomy of privacy issues leads to a number of issues to examine for each of our mOSNs. Some of these have been examined in previous work for traditional OSNs, but bear re-examination for mOSNs, while other issues are raised due to new features of mOSNs.

Availability of user information within mOSNs: What pieces of information are supplied by users for each of the mOSNs and what are the default privacy settings for their availability to others within an mOSN?

Location and presence: How is the availability of a user's location and presence handled by each mOSN?

Interconnectedness of mOSNs: To what degree do mOSNs have interconnections based on API connections with other OSNs, thereby potentially allowing the leakage of information to users in these other OSNs?

Leakage to third-parties: Beyond leakage of information within or across OSNs, to what extent is information about a user leaked to third-parties and does it differ across the various interfaces of each mOSN?

Leakage of new PII to third-parties: Are there new pieces of personally identifiable information, such as the unique device identifier of mobile devices, unique to the context of mOSNs that are being leaked to third-parties?

4.3 Methodology

We created accounts on all mOSNs that we studied and observed the private information requested by each mOSN as well as the default and range of availability of this information to other users within the mOSN. We also noted which mOSNs allow interconnections to be established with other OSNs.

We examined each mOSN from all available interfaces: via a traditional browser of the full Web site, via a mobile browser of the mobile site, and via tailored mobile applications on mobile devices. We used an iPhone device for studying the application behavior of each mOSN because it provides almost complete coverage of our mOSN study set.

Multiple sessions for each interface of each mOSN were used to gather data about possible leakage of private information. The Fiddler [5] Web proxy was used to capture all HTTP request and response headers sent from and received by a Web browser, a mobile Web browser, or an application. We observed that iPhone applications generally use HTTP for communication with a mOSN server thus making it easy for the Web proxy to also capture application traffic. We did observe (via a sniffer) two applications causing some network traffic not passing through the proxy, but were not able to detect any leakage in these cases.

The actions performed within each session are appropriate for the given interface of the mOSN under study; they include: viewing and editing the user's own profile; commenting on other profiles; looking for friends and establishing new ones; checking in to establish location at a particular time, possibly with a comment; reviewing restaurants and attractions; and uploading pictures and tagging them. These actions cover the majority of features provided by the mOSNs in our study set.

5 Results

We used the above methodology to examine all the research issues posed for all mOSNs, and present results. Unless noted, all data were gathered in January 2010.

5.1 Availability of User Information Within mOSNs

Similar to [7], we first examined the availability of pieces of personally identifiable information (PII) in each of the mOSNs. The pieces of PII for a mOSN user include: name (first and last), location (city), zip code, street address, email address, telephone numbers, and photos (both personal and as a set). We also include pieces of information about an individual that are linkable to one of the above: gender, birthday, age or birth year, schools, employer, friends and activities/interests. We only note availability if users are specifically asked for it as part of their mOSN profile.

Results for the 7 mOSNs studied earlier in [7] are largely the same as found at that time except for notable changes by Facebook [1] where name, personal photo, home location, gender and friends are now always available to all other Facebook users if provided by a user. Otherwise privacy settings of these 7 are similar as before and we focus on the 13 mOSNs not previously studied to contrast the level of availability in these newer mOSNs.

Table 1 shows the results of our analysis with the count of mOSNs (out of 13) exhibiting the given degree of availability for each piece of PII (row). The first column indicates the number of mOSNs where the piece of PII is available to all users of the mOSN and the user *cannot* restrict access to it. This piece may also be available to non-users of the OSN—thus a primary source of concern. The second column shows the number of mOSNs where the piece of PII is available to all users in the mOSN via the default privacy settings, but the user can restrict access via these settings. The third column shows the count of mOSNs where there is a piece of PII that users can fill out in their profile, but by default the value is not shown to everyone. The fourth column shows the count of OSNs where a piece of PII is supplied to the mOSN, but not shown in a user's profile. Rows for which the counts do not sum to 13 indicate pieces of PII that are not supplied to all mOSNs.

The rows in Table 1 are shown in the same order as in [7]—sorted in decreasing order of availability. The values in the first two columns raise more privacy concerns (hence the double vertical line) because these show pieces of PII that are always available or available by default. The results in Table 1 show a decrease in availability and thus leakage to other mOSN users similar to [7]. However, we see a smaller core of PII pieces that are always available or available by default—only a personal photo, name, friends and a description of activities are available in the majority of these mOSNs. In contrast, results in [7] show home location, gender, photo set, age/birth year, schools and employer as also available in at least 50% of the OSNs studied. We note that these 13 mOSNs currently request and make available less information about each user in comparison to OSNs previously studied in [7].

Table 1: PII Availability Counts in 13 mOSNs

	Level of Availability			
Piece of PII	Always Available	Available by default	Unavailable by default	Always Unavailable
Personal Photo	10	3	0	0
Home Location	3	4	1	1
Gender	2	3	1	3
Name	5	5	1	2
Friends	6	6	0	1
Activities	3	7	1	0
Photo Set	0	3	0	0
Age/Birth Year	1	3	0	2
Schools	0	1	0	0
Employer	0	0	0	0
Birthday	0	2	0	4
Zip Code	0	0	0	1
Email Address	0	0	1	12
Phone Number	0	0	2	5
Street Address	0	0	0	0

Apart from the availability of different pieces of PII in each of the mOSNs we studied, we observe that settings to control the availability of information are not uniformly available across all interfaces provided by each mOSN. Specifically, each mOSN allows the sharing of information to be controlled by a user via the full Web site interface of the mOSN, but only a minority of these mOSNs provide any privacy controls via the mobile and mobile application interfaces. Thus users accessing a mOSN via a mobile device often do not have ready means to change settings on viewing their information.

5.2 Location and Presence

In contrast to traditional pieces of PII, a new class of information that becomes available in mOSNs deals with a user's current location. A user may "check in" to a mOSN at a particular location via a mobile device, and the location is shared with the user's friends or all users of the mOSN. In some mOSNs a user's location may not be explicitly shown, but may be used to identify nearby places, such as places to eat, for which the user may post public comments for other mOSN users to see. These postings may not identify a user's current location, but can leave a trail of places that a user has visited along with temporal information. Many traditional OSNs also allow users to post timestamped comments, which do not necessarily include location, but do establish a user's presence on the OSN over a period of time. We studied the availability of information for these two actions

across all twenty mOSNs, although we distinguish the results for our set of seven previously-studied traditional OSNs and the thirteen newly-studied special-purpose social networks and the mobile OSNs.

Of the seven traditional OSNs, we find that five provide a means to post public comments and in all of these OSNs, the comments are available by default to all users. For example, postings to a Facebook user's wall or tweets to a Twitter user's public timeline are available by default to all users of these respective OSNs—thus establishing a presence on the OSN that may be seen by other users. However only one of these seven allow for a user to establish a current location—a Twitter user can optionally link a current location with a tweet.

In contrast to these seven OSNs, many of the other 13 treat a user's location as first-class object that is explicitly established and made available for other mOSN users to see. Specifically, three of the mOSNs always make a user's checked-in location available to all other mOSN users and three more make it available by default. Two of the mOSNs make location only available by default to a user's mOSN friends. The rest of the mOSNs may make use of a user's current location, but do not make it available to other users within the mOSN.

The sharing of comments and reviews, which establish presence and may be combined with a location, is provided for in these mOSNs with 4 of them making the comments always available to all users of the mOSN, 7 making them available by default to all mOSN users, one making these comments available to only mOSN friends by default, and one not using public comments.

5.3 Interconnectedness of mOSNs

A unique aspect of the mOSN space relative to traditional OSNs is that rather than exist as independent entities, many of the mOSNs make use of a "connect" API of existing OSNs to extend the reach of a user on each mOSN. Three OSNs—Facebook, Flickr and Twitter—provide such an API interface that is provided as an option to users in other mOSNs. Users of mOSNs can connect their mOSN account with an account on one of these OSNs so that posts, comments and photos on the mOSN become visible on the connected OSN. If we look at the 12 OSNs (other than Flickr and the seven traditional OSNs), eight allow users to connect posts and comments to Facebook, two allow for connections with Flickr, and ten with Twitter.

These connections with other OSNs have privacy implications when the information about a user on one mOSN becomes visible on another OSN. As a specific example, a post including a user's current location on a mOSN that the user has connected to a Facebook account becomes visible on that user's Facebook Wall. As noted above, a user's wall is visible to all Facebook users by default; so even if a user's current location is not visible on the mOSN itself, it may be visible to the millions of users on Facebook. Similarly, Twitter tweets are by default visible to all Twitter users, so locations revealed via mOSN connections have wide default visibility.

5.4 Leakage to Third-Parties

Another type of leakage that we examined for traditional OSNs in [7] is the leakage of private information to third-party servers. This type of leakage can be used to link the browsing behavior of users with actual identity and is independent of any privacy controls provided by a mOSN. As in [7], we observe two types of privacy leakage to third parties: 1) leakage of the unique identifier or userid assigned to each mOSN user; and 2) leakage of specific pieces of PII. Mobile devices also expose a new type of potential PII leakage with mOSNs—the precise location of a user at a given time to a third-party. Unfortunately from a privacy standpoint, we find examples of *all* of these types of leakages in our results. Below, we provide representative examples of PII leakage across each of the interfaces of the mOSNs and conclude this portion of our results with a summary of the third-party PII leakage that we observe.

Figure 3 shows three different mOSN interfaces where the mOSN identifier is leaked to a third-party server as part of a HTTP request via either the Request-URI or the `Referer` header. In each of these cases, this unique id can be used to determine the identity of the user making the request. This is the same type of leakage we found in [7] for traditional OSNs and these examples show it continues across the various interfaces of newer mOSNs.

```
GET /e0?rt=1&amp;...
Host: p.admob.com
Referer: http://buzzd.com/m/buzz/.../id/OSN-ID
Cookie: uuid=ef07qb76f47b19173389f27a9ae1d391
```

(a) Via Referer Field of Buzzd Mobile Web Site

```
GET /pagead/.../profile_restaurants/OSN-ID...
Host: googleads.g.doubleclick.net
Referer: http://www.urbanspoon.com/m/u/add/4
Cookie: id=2015bdfb9ec||...|cs=7aepmsks
```

(b) Via Request-URI of Urbanspoon App Interface

```
GET /openx/www/delivery/lg.php?...referer=
    http://brightkite.com/people/OSN-ID
Host: ad.limbo.com
Referer: http://ad.brightkite.com/openx/www/...
Cookie: OAID=d067746af7039a426ce64147a3201041
```

(c) Via Request-URI of Brightkite Full Web Site

Figure 3: Leakage of mOSN Identifier to a Third-Party

Figure 4 illustrates direct leakage of a user's gender to a admob.com server via the Radar application. Additionally, we see the inclusion of a server-specific header, which is discussed in Section 5.5.

```
GET /ad_source.php?d[gender]=m...
Host: r.admob.com
X-Admob-Isu: IPHONE-UDID
Cookie: uuid=ef07qb76f47b19173389f27a9ae1d391
```

Figure 4: Direct PII Leakage to a Third-Party Via Request-URI of Radar App

A specific piece of information that we looked for being sent to a third-party by mOSNs is a user's current location. An example of such leakage is shown in Figure 5 where the Buzzd app causes the user's location to be leaked as part of the HTTP POST body to pinchmedia.com without any indication to the user.

```
POST http://beacon.pinchmedia.com/
Host: beacon.pinchmedia.com
User-Agent: buzzd/2.2.0 CFNetwork/459
    Darwin/10.0.0d3

beacons="did":"IPHONE-UDID",.."lat":
    "20.00","lon":"-70.00"
```

Figure 5: Location Leakage to a Third-Party Via POST from Buzzd App

Given these specific examples, Table 2 summarizes a count (out of the 20 mOSNs) for leakage of PII to third-party servers via the variety of interfaces provided by each mOSN. These counts are for data re-gathered in May 2010 and largely similar to the original data gathered in January 2010. The last row in the table shows occurrences of location leakage such as the one in Figure 5.

Table 2: Counts of Third-Party Privacy Leakage via mOSN Interfaces

What is Leaked?	Leakage Interface		
	Mobile	App	Full
OSN Identifier	6	2	18
Piece of PII	1	2	5
Location	0	2	0

There are notable observations from Table 2. First, leakage of the OSN identifier via the full Web site interface is widespread and confirms results reported in [7]. Second, generally less observed leakage is found via the mobile Web site and application interfaces. Finally, 19 of the 20 mOSNs exhibit some type of leakage to a third-party with only Loopt having no observed leakage.

In Figure 5 and Table 2 we show an example and occurrence count for location leakage to a third-party. Another scenario also occurs where a user's location is passed to a third-party. This scenario is shown in Figure 6 where the Foursquare application passes the user's latitude and longitude to the Google map service to show the user's current location. While seeing the map may be consistent with user expectations, the user may not be aware that the location has been shared with more than just Foursquare. In our data, we observe that the location is shared with a map service by the application interface of eight mOSNs, the mobile Web site of four mOSNs and the full Web site of one mOSN.

```
GET /maps/vp...vp=20.00,-70.00
Host: maps.google.com
Referer: http://foursquare.com/venue/xxxxxx
```

Figure 6: Current Location Passed to a Third-Party Map Service Via Request-URI of Foursquare App

We can also examine the nature of each type of leakage. While we do not know if the leakage is accidental or deliberate, we can distinguish whether the information is *explicitly* leaked to a third-party by a mOSN via the Request-URI or POST request (examples in Figures 3(b), 3(c), 4, 5 and 6) or *implicitly* leaked via the Referer or Cookie HTTP headers as a byproduct of the HTTP request (as in Figure 3(a)). We observe explicit leakage of the OSN identifier for 9 of the 26 instances in the first row of Table 2. All instances of leakage for specific pieces of PII and location are explicit.

Another notable observation can be made by combining these results with those presented in Section 5.3. Due to the connected nature of this new breed of mOSNs with traditional OSNs such as Facebook and Twitter, it is not just that information such as current location is shared with these OSNs, but the third-parties that know a user's OSN identifier also have potential access.

5.5 Leakage of New PII to Third-Parties

The final vector of privacy leakage that we examined was the leakage of additional pieces of PII to third-parties. One such piece is the unique device identifier, UDID, on the iPhone platform, which could be used by third-parties to track the actions of a user using a device across different applications. Not only does the request in Figure 4 show direct PII leakage, but it allows the admob.com domain (acquisition by Google announced in November 2009) to associate user information with the device identifier and cookie. Similarly, the UDID is leaked along with location to a pinchmedia.com server in Figure 5.

Figure 7 shows a request where the Wattpad application causes the UDID to be passed to the `mobclix.com` domain. In our trace, we observe a subsequent request, caused by this `mobclix.com` server, to a `doubleclick.net` server, which is then in a position to link the UDID to an OSN identifier, such as the Urbanspoon identifier shown in Figure 3(b).

```
GET /?i=xxxxxxxx-xxxx-...&u=IPHONE-UDID&
Host: ads.mobclix.com
User-Agent: Wattpad/1.6.1 CFNetwork/459
    Darwin/10.0.0d3
```

Figure 7: UDID Leakage to a Third-Party Via Request-URI of Wattpad App

Overall, we observed leakage of the UDID to a third-party from an application for six of our mOSNs—in all cases the leakage was explicit. These mOSNS are Buzzd, Brightkite, Dopplr, Flickr, Loopt and Wattpad. The inclusion of Loopt is also notable as we now observe some type of private information leakage from *all* 20 of the mOSNs in our study.

6 Summary and Future Work

In examining privacy leakage in mobile OSNs we have learned that many of the problems in traditional OSNs continue and new ones have been introduced along with the new features. Chief among them is the concern of information leakage from mOSNs to users in traditional OSNs. We examined a broad cross section of popular mobile OSNs and all of them leaked some form of private information. The popularity of location-based, dynamic interaction—a key distinction of mOSNs—is also a potential source of privacy leakage. The combination of location information, unique identifiers of devices, and traditional leakage of other PII all conspire against protection of a user's privacy. Facebook has proposed rolling out a location feature but the way in which it will work with desktop and mobile versions is not yet clear.

The problem of privacy protection for a user is also multi-dimensional as the user must be aware of which users within the mOSN may see private information the duration of a privacy setting, whether information is shared to connected OSNs, which users within those OSNs may see the information, and whether information is made available to third-parties.

Aggregators who are tracking users can now paint a truly comprehensive and dynamic picture of a mOSN user. This picture argues for a comprehensive way to capture the entire gamut of privacy controls into a single unified framework that is also simple enough for users to understand—an inherently difficult proposition.

Moving forward, it is important to continue to monitor potential privacy issues as mOSNs evolve with new features. We are planning to extend our study to other device application platforms and to examine privacy implications of mobility for more than just mOSNs. We are also exploring possible protection measures that encompass the new challenges identified here; one avenue is displaying the set of Internet entities that have access to a OSN user's information at any given time and possible ways of suppressing future leakage of that information.

Acknowledgments

We thank Konstantin Naryshkin for assistance in gathering data for our set of mOSNs and the anonymous reviewers for their helpful comments.

References

[1] Kevin Bankston. Facebook's new privacy changes: The good, the bad, and the ugly, December 9th 2009. `http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly`.

[2] Facebook mobile: 100 million and growing. `http://blog.facebook.com/blog.php?post=297879717130`.

[3] Chari et al. Web 2.0 security and privacy, December 2008. `http://www.enisa.europa.eu/act/it/oar/web2sec/report/at_download/fullReport`.

[4] Regulator warns of mobile Internet privacy concerns, 2008. `http://www.euractiv.com/en/infosociety/regulator-warns-mobile-internet-privacy-concerns/article-172783`.

[5] Fiddler web debugging proxy. `http://www.fiddler2.com/fiddler2/`.

[6] Balachander Krishnamurthy and Craig E. Wills. Characterizing privacy in online social networks. In *WOSN*, August 2008.

[7] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. In *WOSN*, August 2009.

[8] Giuseppe Lugano. Mobile social networking in theory and practice. *First Monday*, 13(11), November 2008.

[9] Global faces and networked places, March 2009. `http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf`.

[10] Please rob me. `http://pleaserobme.com`.

[11] Quantcast mobile web trends, January 2010. `http://www.quantcast.com/docs/download/attachments/3080958/QC_Mob_2009r11.pdf?version=2`.

[12] Jerry Rocha. Mobile next, social networks and applications innovation in mobile, 2009. `http://www.slideshare.net/jerryrocha/ces-2009-mobile-next-social-networks-and-applications-innovation-in-mobile-presentation`.

[13] M. G. Siegler. Location is the missing link between social networks and the real world, November 2009. `http://www.techcrunch.com/2009/11/18/location-is-the-missing-link-between-social-networks-and-the-real-world`.