Locality and Privacy in People-Nearby Applications

Eran Toch
Tel Aviv University
Tel Aviv 6997801, Israel
erant@post.tau.ac.il

Inbal Levi
Tel Aviv University
Tel Aviv 6997801, Israel
inballe2@post.tau.ac.il

ABSTRACT
People-Nearby applications are becoming a popular way for individuals to search for new social relations in their physical vicinity. This paper presents the results of a qualitative study, based on 25 interviews, examining how privacy and locality are managed in these applications. We describe how location is used as a grounding mechanism, providing a platform for honest and truthful signals in the challenging process of forming new social relations. We discuss our findings by suggesting theoretical frameworks that can be used to analyze the social space induced by the applications, as well as to inform the design of new technologies that foster the creation of new social ties.

Author Keywords
People-Nearby Applications, Location-Based Social Networks, Privacy, Security, Qualitative Study

ACM Classification Keywords
H.5.2 Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
Ubiquitous computing is playing an increasing role in the dynamics of creating new social relations. One of the prominent examples is the emergence of mobile applications that enable people to discover and meet new people in their physical vicinity. These applications, which we label "People-Nearby" applications, are the focus of this study. **PNAs (People-Nearby Applications)** are gaining popularity and are used in various contexts such as dating (e.g., Grindr or Skout) or finding activity partners (Highlight or Circle). Unlike location-sharing services that allow location sharing between existing social relations (e.g., Foursquare and Facebook Places), the objective of PNAs is to enable users to meet new people and to form new social relations.

Almost all PNAs provide users with a similar user experience: a directory interface that shows the profiles of individuals ordered by their physical proximity to the user (e.g., how far are they from the user,) a profile page in which users present themselves, and a chat system that enables users to interact with each other. The technical framework is quite standard as well: the application tracks the user's location using the mobile operating system API, transmits the location to a centralized server, allowing other mobile clients to query the server for the location of nearby users. These applications draw great interest from users: Badoo proclaims to have 175 million users[1]; Skout is reported to sign about 1 million new users every month [9], and Grindr, an application oriented towards homosexual men, proclaims to have 4.1 million registered users in 192 countries in April 2011, with users logging on to the service 8 times a day on average[2]. Grindr, for example, seems popular enough at times that some news reports claim that it crashed in the U.K. when athletes arrived at the 2012 Olympic games [5].

Creating a new social relation is an action that combines high gain with high risk, with the potential for social embarrassment, emotional harm and physical risk [26]. The recent reports regarding sexual assaults on Skout [28] demonstrate the tangibility of this risk. In applications that combine virtual and physical interaction between users, these risks are amplified, and are joined by online privacy risks [4]. Therefore, to understand the PNA user experience, we need to understand how users navigate between risk and opportunity. Specifically, we ask the following questions: How do users balance privacy and disclosure in these systems? How do users gain trust in one another? And what is the role of locality in the user experience of these systems?

This paper makes two main contributions to the literature. First, we provide a qualitative analysis of usage patterns in PNAs, based on in-depth interviews of 25 users. We demonstrate how location clues are playing a role in the process of forming new social ties, and how trust is built, preserved and perceived by users. Privacy is a pivotal aspect of location-based systems (LBS) in general, but it is particularly complicated in PNAs as users need to disclose information about themselves to introduce themselves to other users. We analyze the dynamics of privacy, and discuss how self-presentation serves privacy strategies.

Our second contribution is theoretical. We augment the concept of *hybrid ecology*, introduced by Crabtree and Rod-

UbiComp'13, September 8–12, 2013, Zurich, Switzerland.

http://dx.doi.org/10.1145/2493432.2493485

[1]Badoo website: http://badoo.com
[2]Interview with Grindr co-founder Scott Lewallen, conducted by the author at April, 2011.

den [7] with specific reference to privacy and trust in public environments. We demonstrate how boundary regulation processes in hybrid ecologies are connecting the physical realm [1] with the digital realm [25]. Beyond these contributions, we wish to introduce PNAs to the research community. These systems provide an example of real-world applications, with large-scale use, that raise fascinating research questions. Their unique interaction features can make them a useful model for future technologies that enable complex social environments through combined digital and physical interaction.

RELATED WORKS

We identify three central domains for this work: privacy in location-based social applications, computer-mediated methods for social tie creation, and interaction in mixed digital and physical modalities. We position People-Nearby application analysis in the intersection between these two domains.

Privacy in location-based social applications was thoroughly studied in the literature of ubiquitous computing. Studies looked at location disclosure decision-making with different social relations, such as co-workers, friends and family, and in different usage contexts [6]. Further empirical works include quantitative analysis of the intrinsic privacy perceptions of particular places [30] and qualitative analysis of the dynamics of location tracking in the family [3]. The growing popularity of location-sharing applications made it possible to empirically explore emerging usage practices in the real world. For example, Cramer et al. explore check-in practices on Foursquare, a popular location-sharing application, analyzing how sharing norms evolve through conflict and context [8]. Lindqvist et al. describe the various usage practices around Foursquare, focusing on how privacy concerns are managed and handled by Foursquare users [20]. Our work extends these research efforts by focusing on location-based applications that are primarily used to meet new people r.p.m.r than to interact with existing social relations. While Lindqvist et al. documented the fact that some people use Foursquare to meet new people, they found it to be a relatively minor usage practice [20].

The use of computer-mediated communication (CMC) to facilitate initial interactions has been studied in several types of systems [2]. Tidwell and Walther investigated how CMC partners use certain language-based strategies to reduce uncertainty [29]. They found that CMC users utilize disclosure and question-asking strategies that can effectively lead to greater attributional confidence and perceived conversation effectiveness. Gibbs et al. found that self-disclosure on dating sites is an important predictor of perceived relational success [13]. Our effort complements these works by focusing on location as the central principle of PNAs, and therefore in meeting new people though mobile applications. We argue that locality fundamentally changes the way people present themselves and interact with others through these applications.

As People-Nearby Applications function as sociability hubs in a physical space, we need to look at existing relations between the physical environment and and trust. Establishing trust is a key process in urban spaces, where people are need to establish mechanisms to be around strangers. For example, people create social rules and enforce social norms that enable what Lehtonen and Maenpaa define as street sociability [17]. For example, locality can allow the creation of subtle social relations, such as the 'familiar stranger', which provide people with a sense of familiarity with those around them [27].

To understand People-Nearby applications we need to understand the *ecology* of the system. The concept of ecology describes the interaction space induced by a system, which is a structure of people, practices, technologies, and values. Crabtree and Rodden [7] define ecology as "*the space or environment that cooperation takes place within and to the socially organized ways in which the environment affords collaboration.*" The concept of ecology originates from the domain of computer-supported cooperative work (CSCW) to analyze team collaboration [22], and has since spread to ubiquitous computing through the concept of hybrid ecology. Hybrid ecologies merge the physical and digital aspects of a system, leading to fragmented interaction, which is mediated by mechanisms that are distributed between the digital and the physical spaces.

Hybrid ecologies were researched in systems that include tight interplay between physical and digital modalities, such as location-based gaming [19] and location-based social networks [10]. For example, hybrid ecology is used to describe how gamers, playing the 'Dragon Quest 9' proximity sensitive game, interact with each other in an urban environment [19] and how location-sharing applications, such as Foursquare, requires users to take into account spatial and digital cues [18]. In this work, we apply the concept of hybrid ecology to PNAs, as it provides a framework for analyzing the relations between the applications' information design and the social environment induced by users' practices and norms. Our work is focused on spaces that enable people to form new social relations, a process that may introduce very different constraints on privacy and trust than other types of applications.

PEOPLE-NEARBY APPLICATIONS

We formally define PNAs (People-Nearby applications) as *mobile* systems that allow users to discover *new* people using *geographical proximity* search and *online communication*. This definition applies to several applications, including Skout, Grindr, Badoo, Highlight, Circle and many others in the iOS and Android mobile operating systems. Our definition does not include friend-finders applications, which provide location sharing primarily among existing social relations (e.g., Foursquare, Facebook Places or Loopt). In contrast, we focus on applications that are not targeted at creating an explicit online social network, but that provide general means of communication between strangers.

Several dating and job-seeking services allow users to search for people according to their city or address. However, we

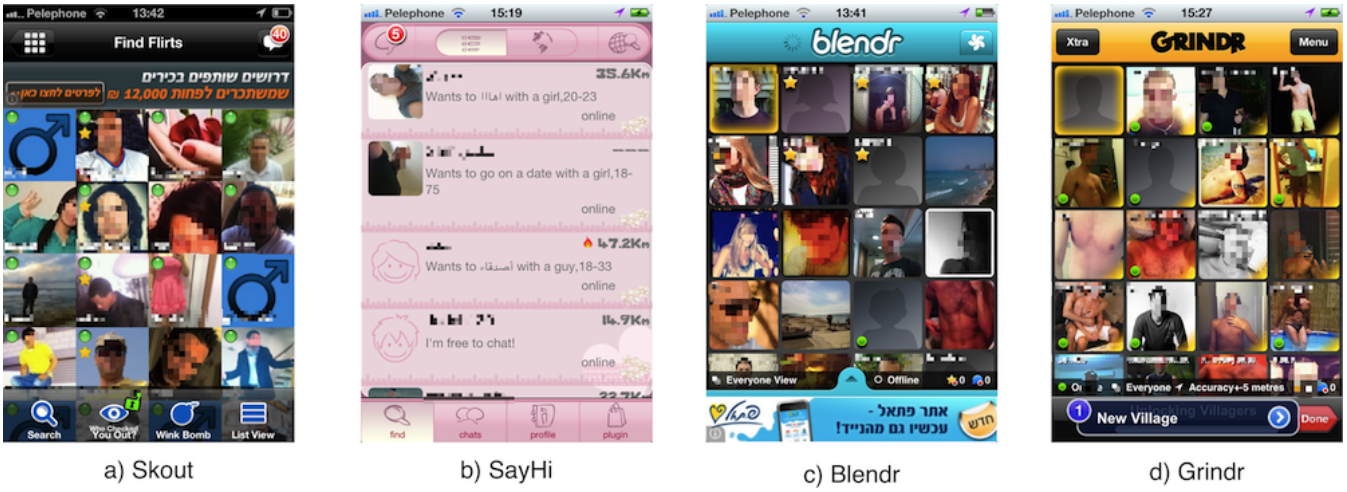

Figure 1. The landing pages of four People-Nearby applications. The faces and names of users were obfuscated to increase anonymity.

are interested in mobile applications that use location as the primary means of discovery, and that use the location tracking offered by mobile operating system platforms. From this definition, the basic mechanisms of PNAs can be easily derived: a People-Nearby application needs to have some sort of a location-based directory for searching for other users, a profile component that allows users to display information about themselves and some sort of a communication mechanism that facilitates interaction between users.

Features of People-Nearby Applications

Figure 1 depicts the screenshots of the landing pages of four PNAs, visualizing the simple set of design guidelines followed by most of these applications. The landing page includes a directory of nearby users, ordered according to the proximity to the user. The directory is displayed as a grid of pictures and names (e.g., in Skout, Blendr and Grindr) or as a list (e.g., SayHi, Circle and Highlight). After selecting a user from the directory, the application displays the user's profile, which includes a set of photos, personal information (e.g., name, age), and other elements that resemble online social networks (e.g., a list of interests, status message and preferred activities). The profile page also displays the user's location, in varying resolutions that can include the exact location of the users (displayed on a map,) a street-level resolution, a city resolution, or just the distance from the user performing the search. Some applications, such as Skout and Badoo, display the current status of the user (online or offline) using a visual notification in the search interfaces (usually a small icon.) Communication with the user is carried out using a simple asynchronous chat system, which is an integral part of all the reviewed applications.

Table 1 describes the properties of several prominent PNAs. The list of application was constructed by searching app stores for the most popular applications, according to the number of downloads estimation and the number of raters. The table describes the applications' objectives, as manifested on the app store. The objectives range between a single straightforward objective (i.e., Grindr's "Find local gay, bi and curious guys for dating or friends for free") to open-ended objectives (i.e. Highlight's "Fun, simple way to learn more about the people around you.") When applications try to appeal to new users in the app-store, their description normally revolves around the idea of locality and physical proximity, as opposed to other types of social networks. The application's description mostly emphasizes the possibility of meeting new people and the opportunity of chance encounters with existing contacts.

User Profiles and Identities

The way users construct their online profile, the information it contains and the way it is presented, structure the boundaries of the interaction within the system. The applications use two dominant strategies in constructing user profiles: allowing free-form profiles or relying on existing social networks for identity management (Facebook, mostly). In free-form profiles, the users create new accounts, entering as much information as they desire, as long as the registration-mandatory information is entered. Table 1 describes the registration mandatory information for each application, ranging from Grindr, where the user is not required to enter any mandatory information except a nickname, to Circle, which relies on Facebook for user identification, and displays information from the user's Facebook profile. What could be the reasons for limiting registration information? According to the head designer of Grindr, this decision was made: *"To avoid patronizing the users. To make them feel that they have more control."*[3]

The identity in many PNAs is effectively pseudonymous, for free-form profiles, and fully-identifiable, for social network-based profiles. In pseudonymous applications, the nickname identifies the person in the application, but can differ from his or her original or true name. Table 1 illustrates the variability of norms surrounding anonymity and self-presentation in PNAs, by analyzing how profile pictures are constructed.

[3]Interview with Grindr co-founder Scott Lewallen, conducted by the author at April, 2011.

App Name	App-Store Description	Registration Mandatory Info	% Clear Picture	Controlling location visibility	No. Raters
Badoo	Badoo is a social network where you can meet new people.	Email, name, age, gender, sexual orientation	49%	Reciprocal location blocking	18,859
Banjo	Banjo integrates the largest social networks to provide on-the-ground view.	Facebook login	80%	Location blocking	1,075
Blendr	The new way to make friends nearby.	Birth date	30%	Hiding location and controlling resolution	2,004
Circle	Social Radar to find your friends and contacts that are nearby.	Facebook login	100%	No location visibility control	5,847
Highlight	Fun, simple way to learn more about the people around you.	Facebook login	100%	Controlling background location monitoring	773
Grindr	Grindr is the essential location-based app to meet gay, bi and curious guys for dating, socializing and friendship.	Nickname	20%	Hiding user distance	97,582
SayHi	SayHi can help you find new people nearby!	Nickname, sexual orientation, birth date	10	Controlling background location monitoring	3,067
Skout	Instantly meet people near you or around the world.	Sexual orientation, search radius	30%	No location visibility control	134,215

Table 1. A list of prominent PNAs. The application-store description column includes the first line of the application's self description, as displayed at the app-store. The registration data column contains the mandatory information. % Clear Picture is the proportion of users with potentially recognizable profile pictures. No. Raters is the number of people who provided app-store ratings for the application.

The percent of clear profile pictures reflects the proportion of user profiles that exhibit a clear and potentially recognizable picture. The criteria for counting a user profile as recognizable included the following: that the photo is of a person (rather than an animal or an object), that the entire face is visible, that the face is not obstructed by sun-glasses or a serious form of obstruction, and that the picture is not of a well-known celebrity. The evaluation was done by assessing each profile picture of all the users in the same state with the interviewer.

To understand the structural properties of the applications, we need to look at privacy controls and sharing mechanisms. Some applications, such as Blendr, allow users to control whether other users can see their location and the resolution of the location (choosing between street, city, or country resolution.) Badoo allows users to hide their location but in a reciprocal manner, hiding the location of other users from users who choose to opt-out. Most applications, such as Badoo, Skout, Grindr, Circle, provide ways to block other users (prevent them from further contact) or providing a way to report the user for inappropriate behavior.

Study Applications

To gain in-depth understanding on People-Nearby application usage practices, we interviewed users of three applications: Skout, Blendr, and SayHi[4]. We chose these applications as they are relatively prominent and popular in Israel in terms of the number of online users. The three applications provide the same set of features: a geographical proximity-based search interface with online status notifications, an online profile that contains pictures, and an embedded chat system. While the services are similar on the technical level, the community of users behave quite differently. The difference between the applications rely on their intended use. Skout is targeted mainly to dating, as its application icon suggests[5] as well as the mandatory information it collects at the registration process (e.g., sexual orientation), and as our participants confirm. SayHi and Blendr are targeted towards a more general use, and therefore offered us a view into other usage patterns in other contexts.

METHODOLOGY

We recruited participants by posting messages using the PNA systems. We sent message to participants who were in the vicinity of the interviewer, which was located in the Tel Aviv metropolitan area. In the applications we surveyed, accessible users were located in the same state as the interviewer, roughly 100 KM or less from the interviewer. Overall, 320 users were invited to participate in the study. Twenty percent of these users returned our messages, and 50% of these people were willing to be interviewed for the research. Five of the interviews were abandoned by the participant at the beginning of the interview and were discarded. Altogether, we interviewed 25 participants. All interviews were conducted in the Hebrew language, and took between 35 minutes and 70 minutes. Five of the interviews were halted by the participants and were resumed the following day after the interviewer had initiated contact with the participants.

The information about the participants is summarized in Table 2. Of these participants, 18 were males and 7 were females. 19 of the participants were native Hebrew speakers and the rest were native Arabic speakers (though all participants were fluent in Hebrew). Fifteen of the participants were from the Tel Aviv metropolitan area. The rest were from peripheral cities and towns in Israel. 19 participants were Skout users, 3 were using Blendr and 3 were using SayHi.

While the acceptance rate for participation is relatively low

[4]We were unsuccessful in recruiting participants on Grindr.

[5]An icon displaying pink heart, at the time of the study.

compared to offline interviews, it is normal for voluntary surveys conducted over the Web [15, 12]. It is important to note, however, that the participation rate introduced a bias towards extravert participants and possibly towards ones with lower privacy concerns. Furthermore, the rejection rate was higher with female candidates, introducing a bias towards masculine approaches and perceptions.

Participant	Gender	Age	Months	Application
P1	M	25-30	1	Skout
P2	M	20-25	-	Skout
P3	**F**	20-25	6	Skout
P4	**F**	25-30	1	Skout
P5	M	20-25	1	Skout
P6	M	25-30	12	Skout
P7	M	25-30	6	Blendr
P8	**F**	35-40	18	Blendr
P9	M	-	3	SayHi
P10	M	25-30	30	Skout
P11	M	25-30	-	Skout
P12	M	25-30	1	Skout
P13	M	35-40	-	SayHi
P14	M	35-40	-	SayHi
P15	M	30-34	1	Skout
P16	M	20-25	12	Skout
P17	M	20-25	18	Skout
P18	M	-	1	Blendr
P19	**F**	35-40	1	Skout
P20	M	30-35	4	Skout
P21	**F**	20-25	2	Skout
P22	M	-	6	Skout
P23	**F**	25-30	3	Skout
P24	**F**	-	3	Skout
P25	M	25-30	1	Skout

Table 2. The demographics of the study participants: gender, age-range, number of months using the application, and the primary application used by the participant. Four participants declined to provide their age and four participants did not say how many months they are using the application.

The interview data was analyzed using the grounded approach [14]. After the interviews were fully transcribed, two researchers together iteratively developed a codebook and coded the data. We then used this coded data to identify themes across categories. We identified themes that are relevant to the main uses of PNAs according to our participants: the usage of specific features, the role of the features in managing both concerns around privacy and identity management and the need to reach and interact with people. The relevant quotes were translated from Hebrew to English for the purpose of publication.

USE OF PEOPLE-NEARBY APPLICATIONS

In this section we explore why and how people use PNAs. We focus on the physical location as the pivotal feature of the applications and investigate the different ways in which location is used and applied. We highlight the most commonly mentioned features: location usage, social interaction, privacy, applicative context and general patterns of usage. Participant numbers are noted after each quote, based on the participant numbers in Table 2.

General Usage Patterns

Why do participants use the applications? When asked about their primary objectives in using the application, 'talking with new people', was mentioned by 14 participants, 'dating' was mentioned by 12 participants, and 'making new friends' was mentioned by 6 participants. The participants reported using their application between two weeks and three years prior to the study, with an average of 6 months and standard deviation of 8 months. The usage frequency varies significantly as well. Participants report on using the application between once a week and several times a day (*"lots"*, as P20 phrased his answer.)

Participants report that the people they meet using the applications are very different than their existing social circle, with regard to socio-economical status and culture. Most of the participants report that the people they talk to are considerably different than the people they regularly interact with using Facebook. Only two of our participants had reported that the people on PNAs are from the same social group as their Facebook friends, and three reported that they are somewhat similar. Six of our participants state that they interact with people in a different language than their own, e.g., Hebrew-speaking users interacting with Arabic-speaking users.

Use of Location

A fundamental aspect of PNAs is the use of location as a way to find and filter people. Indeed, most of the participants perceived location as an important feature in the usage patterns of the majority of participants. Only 4 out of our 25 participants had reported not paying attention to the location of other users. Most users were looking to interact with users that are in their vicinity:

> "Of course that location is important. I want to find someone and meet her, so why should I waste time on just talking? I won't talk with someone who is 200 kilometer away." (P2)

How far away are users looking when searching for other users? The search radius of participants that look for users close by has an average of 50km (with a standard deviation of 20km.) However, the use of location can be sometimes surprising. Six out of 25 participants specifically search for users who are far away, rather than close by. For example, P3 was looking to interact with people from far-away countries: *"I am here to meet people from Asia. I am interested in the Far East."* P12 was looking to talk with people from the U.S: *"I am here mainly to improve my English."* What is the meaning of location to users? Participants report on checking out the city or street of other users to understand the background of other people: *"the location does tell me a little about them, their culture, their perception."* (P21) or to infer the education level of other participants, their nationality and language.

Trust Approaches

Building trust in other users is a challenging and difficult process for many participants. We contextualize the trust issues according to the popular classification of McKnight and Chervany of [23]: trust in the motives of other users and trust in the integrity of other users (and specifically in their identity). Six of our participants report some negative perceptions and feelings regarding the intentions of other users. P21 reports that *"nothing can help me trust people in this application"*, following this with a statement about feeling anxious to meet people through the application. P19 says that her application *"is not particularly safe"* and P3 says that *"I do not believe that you can find someone who can be trusted through this app"*.

Five participants report doubts regarding the integrity of other users: whether their application identity reflects their actual one. For example, P10 says that *"Deception is very easy. Everybody can fill in fake details into their profiles."* and P19 reports that *"everybody wears a mask when they are online"*. The two aspects of trust are overlapping: two participants had reported concerns regarding both the identity of others and their motives. A very small minority of our participants, only three participants, declare that they are either satisfied or unconcerned with regard to their trust with others. Overall, females report lower levels of trust in comparison with males. All 7 females in our study express some negativity regarding trust in other users while only 3 males (out of 18) report similar sentiments. When analyzing the answers, it becomes evident that several participants mix concepts of trust in other application users with trust in the system itself, packing it to a single concept. The three participants that reflect distrust in the system relate it to distrust in other users. For example, one participant states that: *""Everything seems to be fake here. I do not think that I will be able to meet someone here... I do not trust these apps very much."* (P11)

Trust Mechanisms

This challenging trust environment requires users to create mechanisms for uncertainty reduction and to develop norms that encourage trust. Twenty out of the 25 participants in our study report on using at least one mechanism for establishing trust and bridging the divide between them and other users. Four uncertainty reduction mechanisms are signaled out by participants: *location, profile, chat* and *blocking*.

Location is used by 13 of the participants to establish trust in some way or another. The methods can be categorized to two main strategies: location as a grounding mechanism and location as a security buffer. Participants are using the location to ground the hypothetical knowledge about the other userf in some concrete and objective fact. The grounding allows them to know more about the other user, and to reduce the risk in interacting with a stranger. For example, P8 compares the location-based application she is using (Blendr) with previous applications: *"This is a sane application, compared to what happens in others, where you really cannot know anything [about the other person]"*. P7 exemplifies how location provides critical objective knowledge about another person:

> "Knowing the distance kind of helps me trust people. The feeling is that you can trust someone nearby as he or she are not total strangers." (P7)

Users are aware that their location is known to others, and calibrate the information they provide accordingly. This dynamic guides them towards being more truthful, as the location is considered an objective fact sensed by the application itself rather than subjectively reported by strangers. The users are aware of this property, and they actively use the tool to convey and reflect trust, P20 answers:

> "Question: Does location helps you trust other people?
> Answer: Yes, in a sense. Also, because they see where I am. If I am saying that I am somewhere near X and they see that its really so.
> On the other hand, its also possible to use [location] for deception by blocking it on the mobile." (P20)

The last statement by P20 emphasizes the place that location has as a trust-inducing mechanism. Users are wary that automatic location sensing, normally perceived as a robust and neutral mediator, can be rigged. An anecdotal evidence from a Grindr co-founder point to the dynamics of turning off the location: *"in denser cities, people tend to hide their location more often than in a rural area. In rural areas, if you do not have location, people would not be able to locate you."*[6].

The second strategy, location as a security buffer, is used by participants to make sure they are safe when interacting with other users. Four of the participants draw a sense of security from knowing that they are far from the other user. Three participants of the four note that as they do not intend to meet other users face-to-face. For example, P3 objective of interaction depends upon the distance between her and the other user:

> "Question: does the physical location [of the other person] affect your trust?
> Answer: Yes. The further away I am, the more I believe there is no chance of meeting that person." (P3).

Another method for establishing trust is through the users' profile page and chat communication. Five of our participants directly link the user's picture to the trustfulness they feel towards that person. For example, P1 looks for *"girls with a trustworthy picture"*. Four other participants are asking for pictures to establish trust. The use of chat and direct communication also provides participants with a sense of trust. When asked how does he build trust with other users, P7 answers: *"I try to ask a lot of questions, and to request photos to see if the person is trustworthy or not." (P7)*. Users triangulate information from various sources to evaluate the trustfulness of a person:

[6]Interview with Grindr co-founder Scott Lewallen, conducted by the author at April, 2011.

"A profile picture and a picture album mean that the person is actually the person in the picture... Posts, vocabulary and location give an indication for intelligence and trust." (P13).

Finally, blocking and privacy mechanisms are also considered important and useful by four of our participants. For example, one participant describes the process of interacting with another user:

"I ask some basic questions, and I continue to where it takes me. If I see that it [the chat] becomes harassing, I block right away." (P3).

Privacy Management

Participants carefully manage the information available to other people, and the way the profile is structured. Out of 25 participants, 14 had a recognizable picture (one in which the user can be recognized by sight), 6 had a non-recognizable picture (e.g., with sun glasses), and 5 did not have a photo of themselves at all. Only three of the participants had their full name listed on the profile, five of them had only their first name listed, while the rest had used a nickname. The proportion of unrecognizable females was slightly higher than the males, with only 3 out of the 7 females exhibiting a recognizable picture. The participants are wary of providing information that can identify themselves: *"I never give my [phone] number here or my Facebook [page]."* (P3).

Dealing with Harassment

How do users handle intrusions into their virtual space? Seven participants report at least one experience of verbal violence directed at them while using the application. The reports of harassment differ considerably according to gender. 4 out of the 7 female participants report on occasions of violence compared to 3 out of the 18 male participants. While it is impossible to draw general correlations from such a small sample of users, three participants report that women are consistently harassed in the applications. The types of violence is also gender biased. Females complain on receiving unwanted sexually explicit pictures (2 cases) and harassment (sending unwanted and persistent communication - 3 cases). On the other hand, males mention fraudulent communication (1 case) and on acts of racism (2 cases). For example: *"It is clear that there are people in the site who are fake and trying to get money out of you by pretending to be a maiden in distress... or stuff like that" (P13)*

The methods employed by users to counter the harassment are based mainly on the application's blocking and reporting features. The reporting mechanism is mentioned by three users as a crucial element of dealing with violence: *"If you discover that people are fake or perverts you just send the site's team after them [report] and block them..." (P13)* or *"If some pervert harasses me I just block him straight away." (P3)*

Application Usage Context

Users use PNAs in the context of other types of interaction modes and applications. Participants report on a recurring pattern: discovering a person on an application, continuing to communicate by some other means (phone, text messages, instant messaging or Facebook,) and then meeting the person face-to-face. Figure 2 presents the application gateway waterfall: the order of applications used by participants after they use the applications, all the way to the face-to-face meeting. A total of 14 of the participants report of some sort of communication using another method with a person discovered on a People-Nearby application. Out of these 14 participants, 10 are continuing the conversation using the phone, 4 using Skype, 3 using an instant messaging application (namely, Whatsapp), and 2 using Facebook. Seven out of the 25 participants had reported on meeting at least one person they had met on the People-Nearby application.

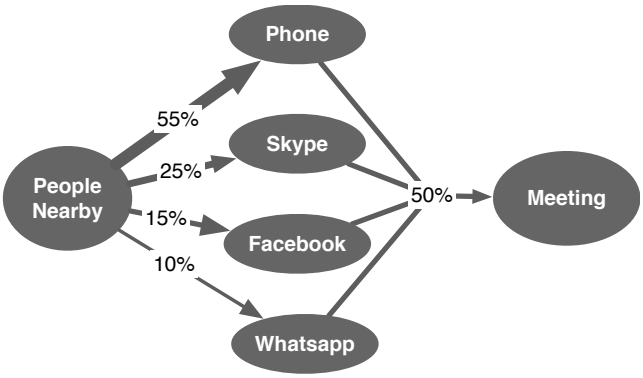

Figure 2. The application gateway waterfall: the methods used for communication after using the People-Nearby application. Percentage is calculated as the proportion out of the 14 participants that report on continuing communication after using the application.

Why do people switch to other communication platforms? For many participants, it seemed like a step forward in an uncertainty reduction process, signaling trust, cohesiveness and access. For example, when a participant was asked on ways to establish trust, she says: *"I move them to Skype, with camera and all that." (P8).* Participants had mentioned being able to see the other person in video, to see more pictures of the other person and to know the other person's phone number as ways to reduce the risk in meeting someone new. Particularly interesting is the use of online social networks such as Facebook. Three of our participants describe how a person's Facebook profile conveys truthfulness. The Facebook profile is treated as an *honest signal*, an identity carrying signal which is very hard to imitate [16]. When a participant (P3) feels unsafe, she makes sure not to provide her phone number or her Facebook profile. One participant explains why:

"Question: How do you make sure that someone is trustful?
Answer: Facebook. You cannot fake pictures with friends, and friends' comments and stuff like that." (P10)

Our participants had constantly drawn comparison between PNAs and more 'ordered' online social networks, primarily Facebook. Facebook is considered an interaction space in which users' identity is fixed and their behavior is regulated.

In contrast, PNAs are less regulated, but as one participant put it, sometimes its part of their charm:

> "There are more normative people here and there are less normative people here... but I think that it's [the application] simplicity is what makes it nice. It's somewhat primitive. Not like those fussy social networks. It's primal." (P8).

DISCUSSION

PNAs present several challenging tradeoffs to their users. They are perceived as a rougher interaction space, marked by the heterogeneous user base, the challenges in establishing trust, and the wide range of usage practices and norms. For many of the participants, these characteristics simultaneously repel and attract. While locality increases the privacy stakes and the risk to users, it is also used to build and encourage trust between users. The pseudonymous profiles, which are the prevalent identity framework in the more popular applications, allow users to experiment and to preserve their privacy. At the same time, pseudonymous identities contribute to a volatile, and sometimes violent, interaction space. Furthermore, PNAs pose several inherent tensions that are seemingly paradoxical. For instance, discovering people in close physical proximity can be perceived as a process that keeps people in their existing social circles. However, our results show that PNAs allow users to interact with people in different social circles and cultures than their own. Running a distance-based search in dense urban areas return heterogeneous results, in a very similar way that a walk in an urban environment will enable interaction with people from different backgrounds. This quality is a divergence from previous models of online social relation forming [26], signaling the ability of locality to provide social diversity rather than homogeneity.

Establishing trust in peers is a multi-stage process in People-Nearby Applications. Most of our participants report on a high level of distrust in other users, and some of them distrust the system itself. The trust-establishing process in PNAs is focused on uncertainty reduction [13], a longitudinal process in which users gain confidence in the identity and intention of their peers. These strategies allow a large proportion of users at the end of the process to trust other users enough to meet them face-to-face. Some strategies rely on internal signals, signals which are controlled by the user, such as constructing the user's pictures and language. Other mechanisms rely on external signals, such as the user's location. One of our main findings is to portray the patterns in which the user's location is used as an honest signal. As the location is controlled by the application, rather than self-reported, it is harder to imitate, and is therefore perceived as an honest signal. Also, our results show the restraining power of application 'policing' signals, such as blocking and reporting. We see that users assume that other users are aware of these features, and take the cooling effect of these features on the whole community.

Uncertainty reduction is a basic strategy in socialization processes, such as online dating [13, 11], and in online social network [16, 26]. However, the ecology of PNAs require users to develop unique uncertainty reduction strategies and mechanisms. First, the use of location information as a grounding mechanism for users' identities. Second, the use of multiple applications, such as Facebook, Skype or text messaging, each revealing a part of the identity of the other user. It is important to note that while previous studies focused on a single application and an exclusive interaction space (e.g., [13, 11, 16, 26], users employ PNAs as a first step in a series of application usage, each signaling an increasing trust and communication intensity. Unlike structured interaction spaces, such as online social networks, most PNAs exhibit a pseudo-anonymized identity schema, where most users remain in obscurity. This range of options can be seen as an example of flexible boundary negotiation process, which is essential for establishing social connections in the online space [1, 25].

The comparison between PNAs and online social networks raises an interesting question: How can we characterize the ecology induced by PNAs? It combines elements from hybrid ecologies, namely the attention users give to both digital signals (e.g., profile information) and physical signals (e.g., location). As Licoppe argues [18], in merging the physical and the digital, users develop strategies for *"spatial reflexivity, in which a sense of the location (or proximity) of self and other in the environment is provided both on screen (through the mediation of mobile technologies) and out of screen (through the embodied resources of the co-present self).* (p. 124). However, the applications require users to function in a hybrid ecology while interacting with strangers, rather than with existing social relations [18] or with other gamers, who share a similar objective [19].

Interacting with strangers in PNAs induces a new kind of ecology, which we name *public-hybrid ecology*. This ecology is characterized by being 'public', in the sense that it is open to users and to different utilizations, and being 'hybrid', in the sense that it combines physical and digital interaction. To unpack the concept of 'public-hyprid ecology', we can point to three specific properties of the interaction space induced by the ecology. First, it is based on anonymity as the default identity framework. Users are free to describe themselves in a relatively free way. Second, it is a multi-purpose space, used for different types of utilization (e.g., talking, dating). This property requires users to interact with people with very different usage practices and norms than themselves. Finally, the space requires some external mechanisms that provide a manageable level of trust and security. These three characteristics create structural constraints and dynamics that users need to navigate in order to reap the benefits of the application. These are *spatial* characteristics, in the sense that they define the virtual geography of the space, the structure and boundaries in which interaction is carried out.

Understanding public-hybrid ecologies requires new models that can be used to analyze the relation between the structural properties of an interaction space and its usage dynamics. Urban studies, a research field of geography and

urban planning is a promising starting point for such models. Urban studies focus on understanding the socio-spatial perspectives of a given space, discovering the relations between geographical properties of a space and its social properties. For example, urban planning scholars observe how the vitality and safety of given neighborhoods are intimately connected to their density and diversity [24]. Similar thinking can be used to uncover the relation between the ecology induced by a social ubiquitous system and the interaction space shared by its users. In our case, it can explain the differences between "regular" online social networks, such as Facebook, and "irregular" people-nearby applications. Facebook works similarly to a private home, regulated by relatively tight social norms and observance. In contrast, PNAs act like a city's public street, exhibiting properties such as anonymity, mixed-use, and risk [21]. Very much like a city street, a good People-Nearby application needs enough diversity and density to make interactions interesting, but at the same time enforced norms that provide safety to its dwellers (i.e., the *block* option.)

Finally, we ask what can PNAs teach us about engaging people in creating new social ties using ubiquitous computing? Scholars such as Wellman [32] and Turkle [31] are arguing that the constant connectivity brought on by ubiquitous technologies are drawing people from their physical environment. This trend can lead to a state in which the urban space is not a "world of strangers" anymore, as Lofland had portrayed the urban environment, with its unlimited opportunities to meet and interact with new people [21]. However, as the dynamics of creating new social relations is radically changing, there is some evidence for the potential of ubiquitous computing to encourage people to meet and interact in the physical space. PNAs, used in social contexts such as dating and making new friends, can be considered early examples of the potential of ubicomp technologies to foster new social ties.

CONCLUSIONS AND FUTURE WORK

In this research, we have begun to explore the ways in which PNAs are used. We have shown the complex and dynamic relationships between knowledge of location and use of that knowledge. We have shown how locality creates a hybrid ecology, changing the expectation of users and grounding interaction in a particular physical context. A close study of a small number of participants does not allow us to generalize about the effect of PNAs on the way social relations are forming; however, it does allow us to lay the foundations for grounded theory. In particular, how the applications form a "public-hybrid ecology" that resemble the virtual edition of a physical public space.

Our analysis points to the mechanisms users find most beneficial. We point to several lessons that can be useful in other types of systems that foster the creation of new social relations. First, our findings point to the many applications users discover for knowledge about location. Users are using location for a multitude of reasons: to understand other users, to gain trust, to convey trust, to feel secure and to filter other users. Location is considered a relatively truthful mechanism, enabling a framework for forming honest signals. It is important to note that location is not synonyms with local, and many users use location to interact with people who are far away.

People-Nearby applications are an example of the potential of open identity and informal trust mechanisms. Most PNAs allow users to manage their identity in an open and flexible manner, while still providing mechanisms to ground knowledge about other users. This architecture may be essential to a user when introducing herself to new social relations. It allows users to maintain their anonymity while observing honest signals that convey trust. Understanding how users use these straightforward mechanisms to establish trust and to maintain privacy, can shed a light on the challenges and opportunities involved in promoting interactions between people.

ACKNOWLEDGMENT

We thank all the participants in the study, who volunteered their time and insight. This work is partially supported by the Israel Science Foundation (ISF) Grant No. 1116/12 and by the Israel Ministry of Science Research Infrastructure Grant No. 3-8709. Finally, we thank Bette Lewis for her editing work and Tali Hatuka for her feedback.

REFERENCES

1. ALTMAN, I. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co., 1975.

2. ANTHEUNIS, M. L., SCHOUTEN, A. P., VALKENBURG, P. M., AND PETER, J. Interactive uncertainty reduction strategies and verbal affection in computer-mediated communication. *Communication Research* (2011).

3. BOESEN, J., RODE, J. A., AND MANCINI, C. The domestic panopticon: location tracking in families. In *Proceedings of the 12th ACM international conference on Ubiquitous computing* (New York, NY, USA, 2010), Ubicomp '10, ACM, pp. 65–74.

4. BRADNER, E., AND MARK, G. Why distance matters: effects on cooperation, persuasion and deception. In *Proceedings of the 2002 ACM conference on Computer supported cooperative work* (2002), ACM, pp. 226–235.

5. BURRA, K. Grindr in london overloaded by gay olympic athletes? *The Huffington Post* (August 23rd 2012).

6. CONSOLOVO, S., SMITH, I., MATTHEWS, T., LAMARCA, A., TABERT, J., AND POWLEDGE, P. Location disclosure to social relations: Why, when, & what people want to share. In *CHI '05* (2005).

7. CRABTREE, A., AND RODDEN, T. Hybrid ecologies: understanding cooperative interaction in emerging physical-digital environments. *Personal and Ubiquitous Computing 12*, 7 (2008), 481–493.

8. CRAMER, H., ROST, M., AND HOLMQUIST, L. E. Performing a check-in: emerging practices, norms and'conflicts' in location-sharing using foursquare. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (2011), ACM, pp. 57–66.

9. CUTLER, K.-M. The story of skout: From deadpoos door to $22M led by Andreessen Horowitz. *TechCrunch* (April 3rd 2012).

10. DE SOUZA E SILVA, A., AND FRITH, J. Locative mobile social networks: Mapping communication and location in urban spaces. *Mobilities 5*, 4 (2010), 485–505.

11. FIORE, A. T., TAYLOR, L. S., ZHONG, X., MENDELSOHN, G., AND CHESHIRE, C. Who's right and who writes: People, profiles, contacts, and replies in online dating. In *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences* (2010), IEEE, pp. 1–10.

12. GARCIA, A. C., STANDLEE, A. I., BECHKOFF, J., AND CUI, Y. Ethnographic approaches to the internet and computer-mediated communication. *Journal of Contemporary Ethnography 38*, 1 (2009), 52–84.

13. GIBBS, J. L., ELLISON, N. B., AND LAI, C.-H. First comes love, then comes google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research 38*, 1 (2011), 70–100.

14. GLASER, B. G., AND STRAUSS, A. L. *The discovery of grounded theory: Strategies for qualitative research*. Aldine de Gruyter, 1967.

15. KONSTAN, J. A., SIMON ROSSER, B., ROSS, M. W., STANTON, J., AND EDWARDS, W. M. The story of subject naught: A cautionary but optimistic tale of internet survey research. *Journal of Computer-Mediated Communication 10*, 2 (2005), 00–00.

16. LAMPE, C. A., ELLISON, N., AND STEINFIELD, C. A familiar face (book): profile elements as signals in an online social network. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2007), ACM, pp. 435–444.

17. LEHTONEN, T.-K., AND MÄENPÄÄ, P. Shopping in the east centre mall. *The shopping experience 1* (1997), 136–165.

18. LICOPPE, C. Merging mobile communication studies and urban research: Mobile locative media, "onscreen encounters" and the reshaping of the interaction order in public places. *Mobile Media and Communication 1*, 1 (2013), 122–128.

19. LICOPPE, C., AND INADA, Y. 'timid encounters': a case study in the use of proximity-based mobile technologies. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems* (2012), ACM, pp. 2759–2768.

20. LINDQVIST, J., CRANSHAW, J., WIESE, J., HONG, J., AND ZIMMERMAN, J. I'm the mayor of my house: examining why people use foursquare-a social-driven location sharing application. In *Proceedings of the 2011 annual conference on Human factors in computing systems* (2011), ACM, pp. 2409–2418.

21. LOFLAND, L. *The public realm: exploring the city's quintessential social territory*. Transaction Publishers, 1998.

22. LUFF, P., HEATH, C., KUZUOKA, H., HINDMARSH, J., YAMAZAKI, K., AND OYAMA, S. Fractured ecologies: creating environments for collaboration. *Human–Computer Interaction 18*, 1-2 (2003), 51–84.

23. MCKNIGHT, D. H., AND CHERVANY, N. L. What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *International journal of electronic commerce 6* (2002), 35–60.

24. NEAL, Z. Seeking common ground: three perspectives on public space. *Urban Design and Planning D*, 0 (2010), 1–8.

25. PALEN, L., AND DOURISH, P. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2003), ACM, pp. 129–136.

26. PARKS, M. R., AND FLOYD, K. Making friends in cyberspace. *Journal of Computer-Mediated Communication 1*, 4 (1996), 0–0.

27. PAULOS, E., AND GOODMAN, E. The familiar stranger: anxiety, comfort, and play in public places. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2004), ACM, pp. 223–230.

28. PERLROTH, N. After rapes involving children, skout, a flirting app, bans minors. New York Times Blog Post, June 12 2012.

29. TIDWELL, L. C., AND WALTHER, J. B. 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 (2002), 317–348.

30. TOCH, E., CRANSHAW, J., DRIELSMA, P. H., TSAI, J. Y., KELLEY, P. G., SPRINGFIELD, J., CRANOR, L., HONG, J., AND SADEH, N. Empirical models of privacy in location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing (Ubicomp'10)* (New York, NY, USA, 2010), ACM, pp. 129–138.

31. TURKLE, S. *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books, 2011.

32. WELLMAN, B. Physical place and cyberplace: The rise of personalized networking. *International Journal of Urban and Regional Research 25*, 227-252 (2001).