
Copyright 2010 Christine Satchell, Marcus Foth, and CHISIG.
Fear and Danger in Nocturnal Urban Environments

Christine Satchell
The Urban Informatics Group
Queensland University of Technology
Interaction Design Group
The University of Melbourne
satch@unimelb.edu.au

Marcus Foth
The Urban Informatics Group
Queensland University of Technology
m.foth@qut.edu.au

ABSTRACT
At the centre of this research is an ethnographic study that saw the researcher embedded within the fabric of inner city life to better understand what characteristics of user activity and interaction could be enhanced by technology. The initial research indicated that the experience of traversing the city after dark unified an otherwise divergent user group through a shared concern for personal safety. Managing this fear and danger represented an important user need. We found that mobile social networking systems are not only integral for bringing people together, they can help in the process of users safely dispersing as well. We conclude however, that at a time when the average iPhone staggers under the weight of a plethora of apps that do everything from acting as a carpenter’s level to a pregnancy predictor, we consider the potential for the functionality of a personal safety device to be embodied within a stand alone artifact.

Author Keywords
The city, convergence, night, privacy, safety, surveillance.

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI).

INTRODUCTION
The open 24/7 model of urban living has reconstructed the nighttime dynamics of inner city spaces. Many once void and abandoned central business districts have become hives of nocturnal activities. Yet there is still only a slim body of research within HCI that looks specifically at the role of technology in mediating physical safety in the streets at night.

In Night and Darkness: Interaction after Dark March et al., (2008) proposes the need to examine night and darkness as a starting point for designing ubiquitous computing. This is a challenge that has recently been addressed by Bloom et al., (2010) whose study of 200 females, identifies the need to alleviate the fear experienced in an urban context, and describes an investigation of a mobile communication system to help meet this need. Relevant research has also been conducted by Blyth et al., (2004) who examines wearable computing technology to help older people overcome fear of crime; Czeski et al., (2010) who explores the potential for technologies to allow parents to monitor teenagers; and in an albeit, less conventional context, the work of Troshynski et al., (2008) into the use of electronic monitoring to keep sex offenders out of defined public spaces. Although coming from different perspectives, these last three papers show that while we want to be protected, we do not necessarily want to be watched. In doing so, the authors raise important concerns about the way in which technologically mediated attempts to ensure personal safety are tightly coupled with surveillance and the erosion of privacy. With this in mind, we explore the concept of personal safety through the critical perspectives provided by the research into privacy. Although our motives for engaging the privacy research diverge from traditional readings in that we exploit the insights for our own pro-surveillance agenda, the result is a critically informed theoretical lens for thinking about the potential technical, social and cultural issues that might arise when harnessing metadata about people for surveillance based purposes.

The first part of this paper describes the context of the research project and summarizes our prior work; the second section explores the relevant literature; and the main part of the paper describes the findings and the design implications that emerged from our ethnographic user study of inner city life. The study was conducted in Melbourne, Australia over a nine-week period. It encompassed approximately 40 hours of ethnographic observation that in turn, generated sixty-seven ad hoc, in situ interviews.

THE RESEARCH PROJECT
The research presented in this paper relates to the second part of a major study conducted for the project Swarms in Urban Villages: New Media Design to Augment Social Networks of Residents in Inner City Developments. The project, which is being conducted over three years, aims to advance the design knowledge of how residents in urban environments can be assisted to communicate and interact through the use of social media to bridge the physical and digital city.

The first user study examined the potential for shared displays and urban screens to enhance a sense of community for inner city residents. Yet, we found the majority of participants to be resistant to urban screens in shared residential spaces. Although this was helpful in contextualizing ‘the non user’ as an important user group whose needs must be addressed (Satchell & Dourish 2009) for the second phase of the research we made a conscious effort to move away from an approach where preconceived technology driven design outcomes were sought. Instead, we set about to understand what problem users were encountering in their everyday urban life that could be addressed with a technological solution. It was from this study that the need to manage fear and personal safety concerns in the city at night emerged.

REVERSE ENGINEERING THE PRIVACY LITERATURE
Palen and Dourish (2003) and Blythe et al., (2004) argue that the pro-surveillance argument needs to be contextualized in light of the potential for systems to produce a dystopian,
Orwellian outcome. Seeing as it is our goal to design technologies that enhance the user’s enjoyment of the city, not increase their paranoia, we take these concerns about surveillance-based technologies seriously.

Palen and Dourish’s work on privacy draws our attention to the well-established digital networks and technological infrastructures that are currently in place. It highlights how social and cultural life requires active participation in this networked world, a world that requires the disclosure of information if one is simply to be a part of it. Furthermore, because these information technologies produce interactions at the intersections of multiple physical and virtual spaces, a culture is evolving where privacy ceases to exist.

Although this process is an inevitable by-product of the digitization of 21st Century life, Palen and Dourish note that a way in which the user might begin to take control is to actively engage in the disclosure of their own information. The data provided by the user becomes their default digital identity and as such, makes access to other, unauthorized information less likely. Therefore, one of the roles of disclosure can ironically be to limit, rather than increase accessibility.

In terms of our own pro-surveillance agenda, this highlights the way in which design considerations cannot be driven solely by what is technically achievable. Rather, they must be considered alongside an understanding of the cultural practices within which the technology will operate. Location and even context based personal metadata can be mapped relatively seamlessly onto pre-existing mobile computing infrastructures. Yet, the gap between technical possibility and cultural barriers can only be overcome if the technology allows for personal disclosure that is managed carefully by the user.

In order to explore the use of surveillance based technologies to empower citizens it is helpful to turn to the concept of ‘sousveillance’. Sousveillance involves the recording of an activity by a participant in the activity; thus, ensuring collective engagement and transparency. Mann et al., (2006) makes the important distinction that unlike surveillance, which often happens in secrecy, tools for sousveillance are freely available and move personal experience capture into the realm of the everyday, with an open forum for public discourse. Furthermore, because sousveillance usually involves a peer-to-peer approach, it further decentralizes observation to produce transparency in all directions.

In summary, the process of reverse engineering the privacy literature set up design process where the technological possibilities were contained by the cultural considerations identified in our user study. As Palen and Dourish note, “What is important is not what the technology does, but rather how it fits into cultural practice”.

THE USER STUDY
The user study observed peoples’ interactions in public and commercial spaces in the inner city of Melbourne, Australia. The aim was to understand what characteristics of inner city life might be enhanced by technology. A mixed methods approach was employed that combined ethnographic observations, augmented with ad hoc, in situ interviews. The research spanned nine weeks. It included approximately 40 hours of ethnographic observation that in turn, generated sixty-seven interviews. The interviews were recorded (where appropriate) using an iPhone and field notes were taken during and immediately after the interview.

As is the case with ethnographic research, an integral part of the process was the act of embedding oneself within the culture of the people, the place and the activities one was researching. Initial sites of interaction included train stations, airport lounges, pubs, shared and solo taxi rides, restaurants, cafés, nightclubs, shopping malls, fast food drive thru, bars, day spas, the supermarket, 24 hour convenience stores, house parties, a dinner party, inner city streets and laneways, mothers group, art gallery exhibition opening, and a dog obedience club.

As mentioned earlier, the study did not set off to examine nocturnal activity, nor did it look specifically at personal safety issues. Rather, this topic emerged through the interview process with 16 of the first 24 participants interviewed citing personal safety concerns as one of the main factors that detracted from the pleasure they got from engaging in activities in the city. In response, the research zeroed in on areas of concentrated nocturnal activity. We were not after the experiences of the lone jogger going for a midnight run in the park, rather we wanted to position our research at the hub of after dark activity. The new focus was on areas such as Chapel St, Prahran, where the late night restaurants, bars, gyms, tanning salons, Internet cafés and 24 hour clubs brought together hundreds of people from all over town.

FINDINGS
The data analysis was conducted using Grounded Theory techniques. It is not within the scope of this paper to provide a full account of the many themes identified in the analysis; instead, we present a synthesized version of our findings. These take the form of cultural considerations and corresponding design implications. We then present three user archetypes to embody the different types of users that emerged from the study and convey a sense of the needs that a personal safety design might have to address.

Cultural Consideration - Fragmentation of Social Networks: The experience of traversing the city after dark unified an otherwise divergent user group through their shared concern for personal safety. Of particular concerns were the solo moments – the time spent either waiting to meet up or dispersing from group based activities. The concern was not only for oneself as an individual, but for the other members of the group one would join, and then be separated from, during the course of the evening.

A main cause of this fragmentation was the way in which the inclusion or exclusion of patrons into late night venues such as Revolver resulted in the artificial and abrupt segregation of groups. The result was that a group of friends that set out to spend the night together, splintered so that some were inside a club, while others where situated in the activity directly outside, with other members commuting between venues, each others houses, or just going home.

Design Implication - Formation of Temporary Nocturnal Networks: Although the parameters of the predefined social networks were eroded, new formations of communities emerged amongst those who were able to get past the rigorous selection process of the door bitch. Participants reported a high degree of trust between individuals previously unknown to each other. Furthermore, the study showed that users were potentially willing to form temporary social networks with people they had just met inside a nightclub with eight participants indicating that they would temporarily augment their mobile social networks with the data generated by these new contacts. The
nature of these bonds was fleeting however, and rarely extended beyond the boundaries of the club.

The study indicated that the temporary networks formed inside clubs could endure and the same networks could reform each Friday or Saturday night. This suggests possible designs for social networking tools to automatically reform these networks in particular circumstances, and capitalize on other possible benefits of networking with familiar strangers (Paulos & Goodman 2003).

Cultural Consideration – Trading Privacy for Security:
Thirty nine of the 43 participants interviewed in the after dark phase of the research reported that mobile social networking platforms digitally mediated a sense of emotional support and security amongst members of real life friendship groups. Thirty-five of the participants saw potential for these networks to be capitalized on to incorporate a sense of physical security amongst friends as they traversed the inner city at night. In order to achieve this, 29 participants reported that they would trade privacy for the security.

Initially, we took this willingness to trade privacy for security as need to repost notions of surveillance within the frame of reference of Gen X and Y, for whom Big Brother is not a dystopian Orwellian force, but rather, a hugely popular reality television show. However, more nuanced questions about the participants attitudes towards privacy highlighted the relevance of the concerns of Palen and Dourish. We found that while users were willing to trade privacy for security this could only be achieved if there were mechanisms in place that would put users in control of shared information and give them the option to not only create new networks but also delete them. For example, 18 users reported that they would use a personal safety device that shared their location on the proviso that the connection was an opt-in function and had a short shelf life. For nine of the users this meant the end of the evening.

Design Implication - Disposable Digital Identities:
An example of how these privacy concerns can be addressed by technology is exemplified by Disposable Maps (Dispomaps). Dispomaps (Seeburger & Schroeter 2009) is an approach to sharing one’s location data in real-time which is visualized on a web based map in a privacy conscious way. Dispomaps allows users to select contacts from their phone’s address book who then receive up-to-date location data. The utilization of peer-to-peer notifications and the application of unique URLs for location storage and presentation enable location sharing whilst ensuring users’ location privacy. In contrast to other location sharing services like Google Latitude, Disposable Maps enables ad hoc location sharing to actively selected location receivers for a fixed period of time in a specific given situation.

Three User Archetypes: Many different archetypes of nocturnal city dwellers were observed interacting with the city, with technology, and with each other. However, the three archetypes presented below were selected because they embody distinct trends to emerge from the study. They illustrate how different groups of people engage, or do not engage, with technology for personal safety issues, and reveal how this impacts on their perception of safety after dark in the city. In addition, these user archetypes were unexpected in that they subverted commonly held notions of vulnerability. Tradition dictates that it might be women who would have the greater fear of the city. For example, Bloom et al., (2010) did not incorporate men in their study. While it is often argued that fear and the perception of danger may encourage women to adhere to gendered social norms of behavior that restrict their independence in public spaces, as we are about to discuss, these very safety concerns can also lead to them being better prepared for dealing with potential danger.

The risk minimizing female urban warrior: Accustomed to adopting a culture of self-protection, members of the risk minimizing female warrior archetype were characterized by a confidence in the city at night that was arrived at by the safety precautions they took. At the centre of these efforts was the avoidance of ending up alone in a deserted and/or dodgy neighborhood. They made sure that they were seen into a cab by their friends and avoided taking public transportation very late at night. Of course, it is not always possible to avoid traversing the seedier parts of town, but even in these situations, the risk minimizing female urban warrior felt protected to some extent because she was armed with the connectivity provided by her mobile phone. This user archetype not only reported how she would call someone in order to deter unwanted attention, she consistently described how these calls were often merely pretence. There was no one on the other end. These faux phone conversations show that the safety afforded by the mobile device could come from the perception of connectivity as well the connectivity itself.

The lone male: We did not set off to use gender as a category for data analysis (Satchell 2010); however, the study found that safety concerns are as prevalent amongst men as they are with women, with almost an equal number of male and female participants citing examples of when they felt unsafe at night. We found that this was largely because gender conventions dictate many moments of late night etiquette and having safely seen his female companion into a taxi, the lone male can often be found on a deserted corner in a questionable neighborhood waiting for the next taxi to come along. Furthermore, the study found that the lone male is acutely aware of the possibility of looming violence. Yet, unlike his risk minimizing female urban warrior counterpart, members of this demographic had little precautionary measures in place for self-protection. For example, only rarely would the he employ the connectivity of a mobile device as a light-weight security measure, rather it was seen as a technology to be reserved for extreme cases such as calling 000 (911) in the aftermath of a personal attack. We did not however, find that this behavior was due to a reluctance by the lone male archetype to use technology in a preemptive manner, so much as the lack of a specific function that enabled this to happen.

The technologically armed sex worker: Of the three archetypes of nocturnal city dwellers we have covered, strippers leaving their place of employment (establishments which were inevitably in the seediest parts of town) reported the least concern for their physical safety. This was because when a club manager could not physically escort them to a taxi or their car, sex workers in the inner city establishments aimed for the reassurance of constant mobile voice contact with co-workers as they left the venue. This helped to minimize the risk of the girls being followed home by patrons of the club. One of the defining features of these calls was that they were made in real time, to real people, and that the person on the move kept up a continual description of their changing location.

Design Implication – Integrating Perceptions of Connectivity with the Protection of Real Time Connections:
We learnt a lot from the digitally mediated personal safety of the sex workers who with their phones glued like a life line to their ear, kept in contact with the club owners or managers until they
made it safely back to their car. They protected their safety and managed their fear by tapping into their real life support group through the use of technology. Unlike the lone male who used technology after a violent incident had occurred, or the risk minimizing female urban warrior who regularly used technology to provide the perception of connectivity, the technologically armed sex worker actually made sure to use mobile technology to harness the power of a network to provide a more practical approach to personal safety.

Although real time interaction with a contact in the vicinity is ideal, the faux phone call and the perception of safety it brings with it should not be discounted. As our study indicated, the perception of safety goes a long way to enhance the feeling of well being in the city at night. Therefore, one of the integral parts of the design would be a mechanism that indicates connectivity. However, the ideal design would be a perception of connectivity grounded in the potential of real time protection via a link to nominated user contacts as well as official security channels such as the police.

DISCUSSION
The technical possibilities for implementing a personal safety mechanism are almost endless; yet, as the process of reverse engineering the privacy literature revealed, the cultural implications provide a means of shaping design outcomes. Our study of nocturnal activity revealed mobile devices are already a major factor in providing users with a sense of security (the risk minimizing female urban warrior) as well as real time protection via the connectivity to a closely co-located person (the technically savvy sex worker). Yet, it could also be seen that the lack of a specifically designated safety function meant that many users (the lone male) over looked the potential of the mobile phone to protect themselves, and to look out for their friends.

The integration of a specifically designated safety function within current mobile social networking platforms is potentially problematic though. An effective safety device is one that transcends functionality and acts a conduit to a culture where groups of people are looking out for each. This is not easily achieved when a new application has to compete for the user’s attention on a functionality rich mobile device. Although our work to date has focused on pre-existing mobile social networking technologies, at a time when the average iPhone staggers under the weight of a plethora of apps that do everything from acting as a carpenter’s level to a pregnancy predictor, we need to consider other approaches for embodying a personal safety device. Despite the trend for convergence, a personal safety device could exist as a stand-alone artifact.

As a stand alone artifact the device would be free from the design constraints of a mobile phone. Blythe et al., (2004) has indicated the potential for the coupling of personal security functionality with wearable technology. Furthermore, a separate entity represents a clean slate users can populate with a set of personalized contacts that they are comfortable displaying and sharing real time locations based information with. Thus, closing the gap between technical possibility and cultural barrier by encouraging personal disclosure that is managed carefully by the user.

CONCLUSION
The focus of HCI is no longer grounded by the notion of the stationary user moored to a fixed PC in an organizational context. Rather, the user is constructed as a fluid, mobile individual who interacts with technologies across a broad range of contexts. Thinking about these interactions and activities as extending past midnight constructs the user in a 24/7 context, allowing a new set of user needs to emerge. We have spent considerable time examining the way in which the promise and the excitement of nightlife in the city is underpinned with an element of unease. We have touched on the possibility of re-contextualizing surveillance so that the connectivity provided by mobile social networks might provide users with greater levels of personal safety. The next step of the research will explore other design solutions. Specifically, we will examine the use of stand-alone security beacons by engineers in remote areas of Australia in order to see if the dialogue they generate about how and when they will be used, makes users more aware of looking out for each other. Thus, contributing to cultural change that would not be possible if the safety aspect was competing with a multitude of other functionalities.

ACKNOWLEDGEMENTS
We would like to acknowledge the ARC for funding this research, the participants in the user study for their valuable insights, the support of our colleagues at the Urban Informatics Group at Queensland University of Technology and The Interaction Design Group at The University of Melbourne, and OzCHI short paper reviewer #3 for his/her suggestion regarding familiar strangers.

REFERENCES
Mann, S., Fung, J. and Lo R. Cyborglogging with camera phones: steps toward equivoivalence. ACM Multimedia ’06.
Satchell, C. and Dourish, P. Beyond the user: use and non-use in HCI. In Proc. OzCHI ’09.