Keeping Information Private in the Mobile Environment

Andrea Grimes, Peter Tarasewich
HCI Laboratory, CCIS, Northeastern University
360 Huntington Avenue, Boston, MA 02115
{agrimes, tarase}@ccs.neu.edu

Christopher Campbell
IBM Almaden Research Laboratory
650 Harry Road, San Jose, California 95120
ccampbel@almaden.ibm.com

ABSTRACT
Protecting the privacy of sensitive information is an important consideration in the design of mobile devices and applications. As computing becomes more pervasive, users are able to access information in places such as airports, stores, and restaurants. When personal information is accessed in such public places, it needs to be shielded from strangers. Techniques are needed for the mobile environment to ensure that sensitive information is kept safe, yet still easily accessible and readily understandable in a variety of contexts. In addition, the user should not be required to actively protect sensitive data, but should feel secure in the fact that the application will automatically protect the data. To this end, the authors have been developing ways to display sensitive information on mobile devices such that it is not readily identifiable to an outside observer. We discuss our work to date, our ongoing investigations, and call for more research into this important aspect of ubiquitous computing.

Keywords
Privacy, context, public places, mobile devices, pixels, information displays, security, ubiquitous computing.

INTRODUCTION
Privacy, while not guaranteed by the US constitution (or those of most countries), is something that most people value and expect, albeit to varying degrees. In today's environment of ubiquitous technologies that monitor people and the flow of information, maintaining privacy becomes more difficult. People do, however, find ways to protect the privacy of their own information and those of other people they may be responsible for. In a fixed environment, like an office, people can control the way that information is handled to minimize the divulgence of sensitive information to unauthorized parties [5]. When the environment is not fixed, and can potentially change in a fraction of a second, the task of privacy management becomes more of a challenge, but one that must be met to ensure the acceptance and viability of ubiquitous computing applications.

Mobile devices play an increasing role in supporting the interactions of our society. Mobile computing has provided people with the opportunity to retrieve e-mail, browse the Web, and perform other tasks in contexts such as shopping malls, sidewalks, and public transportation. Thus, individuals are beginning to access potentially sensitive data such as bank account balances and medical histories in public settings. Because of this, the issue of situational privacy arises: if individuals use mobile devices to access or discuss sensitive data in public places, that data may also be accessible by strangers in their immediate vicinity. Information can also be gleaned and recorded from the myriad of video security cameras that are becoming ubiquitous fixtures in many public spaces. Such situations can have consequences ranging from simple embarrassment, misinformation and rumors to identity theft and monetary loss, among others.

This type of situation can already be seen with cell phone use: more individuals are carrying out private conversations in public, making personal conversations accessible to those in their immediate vicinity [4]. People are using cell phones in places that may not be appropriate for the discussion of sensitive information. When using a cell phone, however, individuals are often not focused on where they are, but on whom they are speaking with. Users of cell phones exist simultaneously in the physical space they occupy and the virtual one for their conversation. A cell phone user must decide which is more important, and bear the consequences of that decision [8]. Often, priority is given to the virtual space. The virtual space can also change quickly (e.g., if someone is walking down the street while speaking on a cell phone). It is difficult for a user to adjust for changes in context when most of their attention is focused on the conservation and the virtual space.

This situation also carries over to the display of information on mobile devices such as PDAs, where people who are co-located with a mobile device user may have unintended access to information that the user is receiving or accessing. This potential vulnerability necessitates the design of information displays with a focus on protecting potentially sensitive information under changing contexts. Otherwise, users must accept certain tradeoffs between the availability of information and the potential loss of privacy and security.

Privacy is a ubiquitous and universal problem that must not only be addressed through privacy policies and data security methods, but also through good user interface design. We believe that tradeoffs between information availability and privacy/security can be minimized through the development of improved information display techniques for mobile devices. Of course, these techniques

must address the limitations of small devices and how users interact with them in a variety of contexts.

USING PIXELS TO AUGMENT PRIVACY

Methods of maintaining data privacy are becoming increasingly important as more personal information is accessible on mobile devices. Work has been done to construct models of interaction that provide computer users with greater control over their privacy [7]. However, such work has focused on the use of an individual's data by remote parties. In contrast, we look at privacy at the point of information display.

Definitions of the exact meaning of privacy vary in their comprehensiveness and focus. Some argue that privacy is a matter of human dignity, while others propose that privacy is more related to personal autonomy [2]. In the context of our work, privacy is viewed as the ability of an individual to access their information while restricting strangers' access to this information. In our recent study [6], issues that arise when individuals access personal information in public settings were examined. Since privacy can vary according to a person's preferences, a questionnaire was administered to determine what types of information individuals generally prefer to keep private. Results showed that subjects felt most strongly about protecting the privacy of medical and financial information.

The results of this questionnaire were used to test the usability of *privacy-augmented* mobile device displays that combined pixels (colored circles) with text in order to maintain desired levels of privacy in otherwise non-private displays. Pixels have been shown to be useful for displaying information (in the form of customizable short messages or notifications) without the need for text, graphics, or even a screen [1, 10, 11, 12]. In this experiment, a handheld device was used to present information in two different contexts, a bank account statement (shown in Figure 1) and information from a hospital visit. In Figure 1, the bank account balance is represented using color while all other information is displayed in plain text.

The results of the experiment indicated that individuals could effectively recognize numeric and other coded data in privacy-augmented displays. The subjects had positive perceptions of such mixed displays for privacy purposes and 75% indicated that they would utilize privacy-augmented text displays on a mobile device. Subjects also said that they would use these types of displays to encode other personal information such as bank account numbers. When asked to indicate which type of information (bank account or health) they considered more private, subjects differed in their responses. This indicates that systems with privacy-augmented displays should allow users to choose which types of information are encoded. Many subjects also commented that if they were able to use their own color mappings, they would be able to interpret the screens even better.

If users can customize their own messages in a pixel-based format, and consistently recognize them when they are displayed, then pixel-based formats can be an effective way of privately and securely displaying information in public places. For example, three green lights on a ring, even when noticed by other people nearby, could convey a message only understood by the wearer. Privacy and security are also automatically addressed during the transmission of such information through public channels, since the mapping of information to pixels can be done before the information is sent, and is user-specific (i.e., not an encrypted message).

Figure 1. Example bank account screen. The bottom four circles are (from left to right) yellow, tan, blue, and magenta and represent the number 1368.

BLINDERS

In addition to color-encoded text, the authors are investigating an alternative method of concealing private information. With *blinders*, sensitive information is hidden by colored tiles. This idea mimics an individual using a blank piece of paper to cover a sensitive document so that it is not viewable by others in the vicinity or using stick-it notes to cover parts of a larger document. Blinders can be used to provide a mixed display in which sensitive information is hidden but information not considered private displayed normally. If the user decides to view a piece of private information, they can temporarily remove the blinder. For example, blinders on a PDA might be removed by touching them with a stylus. When the stylus is removed, the blinders reappear. With blinders, private information is not constantly viewable: it is only shown when the user decides it is safe to do so. This method of providing privacy accounts for the change in context of a user; if a person moves to less public space, they can turn off the blinder feature and view all of their information in plain text. This flexibility allows adaptation to the changing environment of the mobile device user.

CONTEXT ADAPTATION

Context adaptive mobile devices can provide seamless privacy. With blinders, context is an important factor because in less public situations, users may be able to turn off the privacy feature. A truly adaptive mobile system would take into account relevant changes in the user's

environment on a real-time basis and modify the information display as appropriate. While seemingly straightforward in theory, in reality such systems are difficult to implement for a number of reasons. First, determining which context factors are relevant to a user and application at any time is difficult. Second, technologies that adequately sense and process changes in the environment are still under development. Third, one needs to determine if (or how) context information should be used to change the form of information displayed.

There are ways in which context can be used to simplify interaction with an interactive system, including 1) reducing the need for input/action by the user, 2) reducing the quantity of information that has to be processed by the user or increasing the quality of the information presented, and 3) reducing the complexity of rules constituting the mental model of the system [3]. Devices that derive input indirectly from the user or from their surroundings might improve usability in a dynamic environment.

Adaptable systems, however, must still account for the limitations and needs of their human counterparts. When the context changes rapidly, it may be distracting or impractical to adapt to every change [9]. Confusion may also result from incorrect readings of context conditions or a misunderstanding of how changes in context are relevant to the user and/or application.

WHERE DO WE GO FROM HERE?

Privacy is an important design concern when considering the future of mobile devices. When these devices are used in public situations, users run a greater risk of their information being accessed by strangers in their vicinity. The results of our privacy preferences questionnaire showed that individuals are concerned about others viewing information that they consider private. Though protecting data privacy and security during transmission is an important issue that has continued to receive a great amount of attention and research focus, providing information privacy in local contexts is becoming increasingly important as mobile technology becomes more pervasive.

The different types of display privatization methods that we have described in this paper can be summarized as follows:

- Pixels (small display privatization)
- Information reduction (designed display privatization)
- Customization (interactive display privatization)
- Blinders (interactive privatization)
- Context adaptation (intelligent privatization)

One overall question to researchers is which of these methods is the most effective and requires the least effort on the part of the user and on UI designers/developers? There may be some ideal combination of privatization methods, or the methods may depend on the class of information (e.g., financial, medical, social, personal, professional) being secured. Another interesting question is: can designers use the fact that shrinking screen sizes also mean that less information can actually be displayed at one time, thus reducing or changing the information privacy protection needed?

We plan to continue with the study of privacy-enhanced displays that use pixels and other customizable methods to protect users' sensitive information on display screens. Work will continue with blinders as well. Longitudinal tests and field studies will be performed to evaluate the true usefulness of these techniques. A more complex issue is developing ways to measure and use context to determine the level of privacy needed at any given time. This will necessitate the development of algorithms to determine what information needs to be kept private and what can be displayed.

Any privatization method should also take into account who might have access to a user's information. For example:

- Disinterested stranger (e.g., someone accidentally sees a person's PDA)
- Interested stranger (e.g., someone who is trying to see the information but not with any great effort)
- Determined stranger (e.g., stalker or private detective)
- Colleague
- Friend
- Family member

The more common ground (prior information) one shares with another, the more the information needs to be obscured or abstracted for it to remain private. So, for some family members and friends, one may need to keep the information completely out of view.

On a similar note, there may be different ways to display the same information that correspond to different levels of privacy. This would make it easier for users to set privacy policies in terms of "high" or "low" protection levels.

REFERENCES

1. Campbell, C., and P. Tarasewich. Communicating with Three Lights. In Extended *Abstracts of CHI 2004*, ACM Press (2004), 1199-1202.
2. Cavoukian, A., Tapscott, D. *Who Knows? Safeguarding Your Privacy in a Networked World*. McGraw-Hill. New York, NY, USA, 1997.
3. Chevrest, K., N. Davies, K. Mitchell, and C. Efstratiou. Using Context as a Crystal Ball: Rewards and Pitfalls. In *Personal and Ubiquitous Computing*, Springer-Verlag (2001), 8-11.
4. Cooper, G. The mutable mobile: Social theory in the wireless world. In *Wireless World: Social and Interactional Aspects of the Mobile Age,* Springer-Verlag (2002), 19-31.
5. Dourish, P., Grinter, R. E., Delgato de la Flor, J., and Joseph, M. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem.

In *Personal and Ubiquitous Computing 8*, Springer-Verlag (2004), 391-401.

6. Grimes, A. and Tarasewich, P. (2004). Testing Privacy-Augmented Displays on a Mobile Device. Working paper.
7. Hong, J.I., Landay, J.A. An architecture for privacy-sensitive Ubiquitous Computing. In *Proc. MobiSys'04*, ACM Press (2004), 177-184.
8. Palen, Leysia. Mobile Telephony in a Connected Life. In *Communications of the ACM*, *45(3),* ACM Press (2002), 78-82.
9. Schilit, B., N. Adams, and R. Want. Context-Aware Computing Applications. In *Proc. of the Workshop on Mobile Computing Systems and Applications*, IEEE CS Press (1994), 85-90.
10. Tarasewich, P., T. Bhimdi, and M. Dideles. Testing Visual Notification Cues on a Mobile Device. In *Extended Abstracts of CHI 2004*, ACM Press (2004), 1562.
11. Tarasewich, P., and C. Campbell. User Customization of Three-Pixel Displays. In *Extended Abstracts of UbiComp 2004*, Springer-Verlag (2004).
12. Tarasewich, P., C. Campbell, T. Xia, and M. Dideles. Evaluation of Visual Notification Cues for Ubiquitous Computing. In *Proc. of UbiComp 2003*, Springer-Verlag (2003), 349-366.