What Are *You* Looking At?

Peter Tarasewich
HCI Laboratory, CCIS, Northeastern University
360 Huntington Avenue, Boston, MA 02115
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 be easily accessible under a variety of contexts. 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.

1. INTRODUCTION

Mobile devices play an increasing role in supporting the interactions of our society. Users are now capable of accessing information in virtually any sort of public setting, including city streets, buses, restaurants, hotel lobbies, and shopping malls. This creates situations where sensitive information, both organizational and personal in nature, can be seen and captured by people and technology in the immediate vicinity. Maintaining privacy in the mobile environment remains difficult because the context of a device or application can change rapidly and without notice. This is in sharp contrast to a fixed environment, like an office, where people can consistently control the way that information is handled to minimize the chance of divulging sensitive information to unauthorized parties [2].

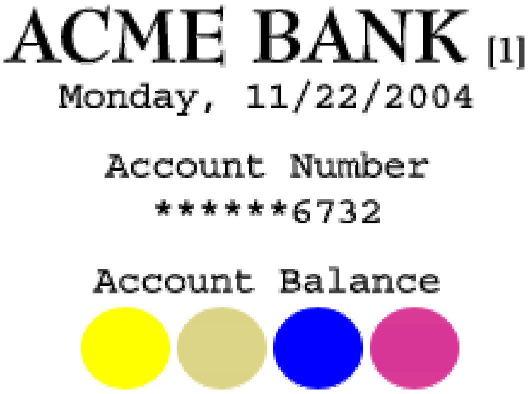
People are not intentionally careless when it comes to protecting information in public places, but social informatics issues make it easy for unsafe conditions to exist. For example, more individuals are using mobile phones in public, making conversations accessible to those in their immediate vicinity. Laptop computers, are also often used whenever and wherever needed or desired (e.g., in a classroom, train terminal, or airplane). In these situations, the user can easily become more focused on the task at hand rather than the fact that information might be overseen, overheard, or recorded by someone close by. While current technology makes it easier to access information anywhere and anytime, it does not do an adequate job of making it easy to protect that information at the same time. Innovations are needed to protect the information that users access on their mobile devices without adding to the existing complexity of the mobile environment. If this is not accomplished, users must accept tradeoffs between the pervasive availability of information and the potential loss of privacy and security [4].

This research looks at the relatively unexplored problem of maintaining the privacy of *displayed* information. Our overall goal is to create technically sound but practical methods of maintaining privacy of sensitive information that is displayed in public and mobile environments. 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. Tradeoffs between information availability and privacy/security can be minimized through the development of improved information display techniques. Of course, these techniques must address the limitations of small devices and how users interact with them, and ultimately solutions should be able to adapt to a user's changing context.

2. USING PIXELS TO AUGMENT PRIVACY

Visual information can be conveyed on small devices (even those without a screen) through the use of *pixel-based displays* [1, 5], which contain one or more individual "dots" (e.g., lights). These dots can have characteristics such as color, intensity, and state (e.g., on/off or blinking). If users customize their own messages in a pixel-based format, then pixel-based formats become 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).

Recently, we tested the concept of *privacy-augmented* displays, which combined pixels with text in order to maintain more desirable levels of privacy in otherwise non-private displays [3]. An experiment was performed with a handheld device that presented information in two different contexts, a bank account statement and information from a hospital visit. Figure 1 shows a bank account balance represented using colored pixels while all other information is displayed in plain text. Results showed that individuals can use pixels to effectively recognize numeric and other coded data, and are positive in their perceptions of such display formats for privacy purposes.



ACME BANK [1]
Monday, 11/22/2004

Account Number
******6732

Account Balance
● ● ● ●

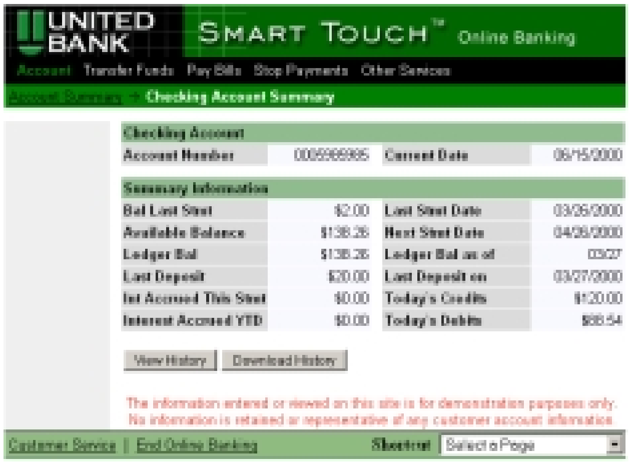
Figure 1. Example bank account screen. The bottom four circles are (from left to right) yellow, tan, blue, and magenta and represent the number 1368.

3. BLINDERS

Our testing to date has shown that user-customized pixels can convey information effectively, privately, and securely. However, pixels still 1) require effort in terms of mapping information to pixel characteristics such as color, 2) require the user to learn these mappings to effectively use them, and 3) can realistically be used only for small amounts of information. Therefore, while we hypothesize that pixel-based privacy-enhanced displays will prove effective for certain applications, it is desirable to investigate alternative techniques that address some of these limitations.

One alternative is the use of *privacy blinders* to conceal private information. With privacy blinders, sensitive information is hidden by opaque squares. This idea mimics using yellow sticky-notes to cover parts of a larger document. Blinders can be used to provide a display in which sensitive information is hidden but other information is visible. To test the effectiveness of privacy blinders, we implemented the technique as a Mozilla FireFox Web browser extension running on a tablet PC. Privacy blinders were generated to appear directly centered over protected information. Users could reveal information in one of two ways. In the first, when the stylus was moved over the privacy blinder, the blinder disappeared and revealed the information underneath it, and reappeared when the stylus was moved away. In the second, when a special stylus gesture was made directly over a blinder, it revealed its information for 10 seconds before reappearing. Additionally, for both implementations, privacy blinders that overlapped one another functioned together in a recursive manner.

For an experiment, a controlled (offline) environment was created for portions of three personal banking Web sites. Figure 2 shows a sample page from one Web site, and Figure 3 shows the same page with privacy blinders enabled. Blinders protected elements such as account numbers and dollar amounts. We collected data on the times that participants spent on information retrieval tasks under each blinder alternative. The average times needed for completing a task using these three alternatives were significantly different. Gesture blinders increased task times when compared to standard blinders, and using either blinder resulted in increased task times compared to using no blinders at all. However, from participant feedback received, such an increase in task times is considered acceptable if it provides a level of privacy that would otherwise not exist.


UNITED BANK
SMART TOUCH™ Online Banking
Account Transfer Funds Pay Bills Stop Payments Other Services
Account Summary → Checking Account Summary

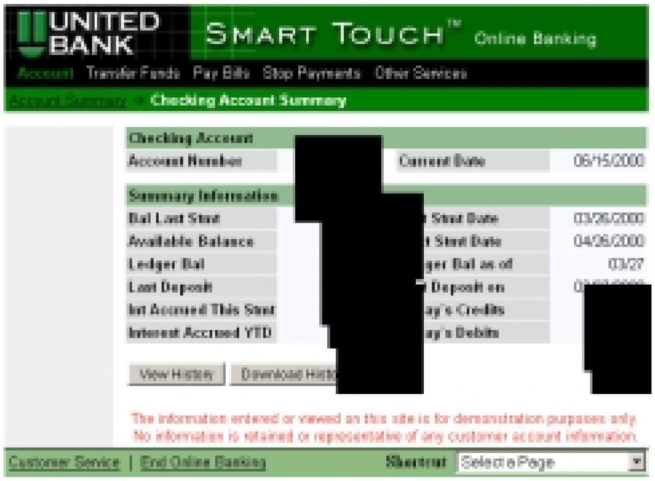
Checking Account			
Account Number	0005989985	Current Date	06/15/2000

Summary Information			
Bal Last Stmt	$2.00	Last Stmt Date	03/26/2000
Available Balance	$138.26	Next Stmt Date	04/26/2000
Ledger Bal	$138.26	Ledger Bal as of	03/27
Last Deposit	$20.00	Last Deposit on	03/27/2000
Int Accrued This Stmt	$0.00	Today's Credits	$120.00
Interest Accrued YTD	$0.00	Today's Debits	$88.54

View History
Download History

The information entered or viewed on this site is for demonstration purposes only. No information is retained or representative of any customer account information.

Figure 2. Personal banking Web site without privacy blinders


UNITED BANK
SMART TOUCH™ Online Banking
Account Transfer Funds Pay Bills Stop Payments Other Services
Account Summary → Checking Account Summary

Checking Account			
Account Number	[redacted]	Current Date	06/15/2000

Summary Information			
Bal Last Stmt	[redacted]	t Stmt Date	03/26/2000
Available Balance	[redacted]	t Stmt Date	04/26/2000
Ledger Bal	[redacted]	ger Bal as of	03/27
Last Deposit	[redacted]	t Deposit on	[redacted]
Int Accrued This Stmt	[redacted]	ay's Credits	[redacted]
Interest Accrued YTD	[redacted]	ay's Debits	[redacted]

The information entered or viewed on this site is for demonstration purposes only. No information is retained or representative of any customer account information.

Figure 3. Personal banking Web site with blinders (account number and balances are protected)

4. WHERE DO WE GO FROM HERE?

Our initial studies show that pixel-augmented displays and privacy blinder methods are viable options for protecting private information in a public setting. For pixels, we need to look further at issues of design and customization. For blinders, we need to investigate appearance (size, color), behavior (control of blinders), and personalization. There may be some ideal combination of privatization methods, or the methods may depend on the class of information (e.g., financial, medical, social, professional) being secured. Longitudinal tests and field studies will be performed to evaluate the true usefulness of these techniques.

Context data might also be used to automatically ensure that a user is interacting with a mobile information system in the safest possible manner, while still allowing for the greatest ease of use. Context data will need to be used in conjunction with privacy preferences, rules, and guidelines from both a user and organizational point of view. A truly adaptive mobile system would take into account relevant changes in the user's environment on a real-time basis and modify privacy management and information display settings as appropriate.

5. REFERENCES

[1] Campbell, C., and P. Tarasewich. What Can You Say With Only Three Pixels? In *Proceedings of Mobile HCI 2004*, Springer-Verlag (2004), 1-12.

[2] 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.

[3] Grimes, A. and Tarasewich, P. (2005). Testing Privacy-Augmented Displays on a Mobile Device. *Proc. of HCII 2005*, to appear.

[4] Hong, J.I., Landay, J.A. An architecture for privacy-sensitive Ubiquitous Computing. In *Proc. MobiSys'04*, ACM Press (2004), 177-184.

[5] Tarasewich, P., C. Campbell, T. Xia, and M. Dideles. Evaluation of Visual Notification Cues for Ubiquitous Computing. In *Proceedings of UbiComp 2003*, Springer-Verlag (2003), 349-366.