Exploring the Perceived Privacy of On-Screen Information and Its Impact on the User Interface Design of a Self-Service Terminal

Elina JOKISUU, Andrew W. D. SMITH and Phil DAY

User-Centred Design, NCR Corporation, Dundee

Abstract. Self-service terminals (SSTs) such as automated teller machines (ATMs), often handle information that is personal and sensitive in nature e.g. financial details. So it is vital that the user feels their information privacy is not compromised by the SST. This exploratory study investigates how users perceive the privacy of an ATM user interface. Using paper prototyping and role-play, the study participants identified those user interface areas they perceived to be the most and least private.

Keywords. Privacy, ATMs, self-service terminals, user interface design.

1. Introduction

Self-service terminals (SSTs) such as automated teller machines (ATMs), are often used in public places by users to enter and view information that is personal and sensitive in nature e.g. financial details and PINs (Personal Identification Numbers). So information privacy is often a significant concern for users and has been identified as one of the key factors influencing a user's decision to use an ATM (Little, 2003). However, an observational field study on users' behaviour when entering their PIN at an ATM revealed that only about 35% of users made any observable effort to secure their PIN. The most common security measure used was hiding the PIN entry with their other hand or wallet (De Luca et al., 2010). Privacy is a real concern. The threat of visual data security breaches, where sensitive personal information is seen, captured and utilised by unauthorised individuals, is constantly rising (Honan 2012). One criminal technique used is known as shoulder-surfing where sensitive data is obtained usually by watching over the shoulder of (or recording) someone entering their PIN at an ATM or at a payment point (Shorter Oxford English Dictionary, 2007). Shoulder-surfing has been studied before but mainly on the challenge of trying to balance good usability with the technical requirements for secure authentication. For example, research has suggested different types of PINs and passwords that would be memorable and easy to enter while being difficult for outsiders to decipher visually (e.g. Tari et al. 2006; Roth et al., 2004; Mahansaria 2009). Brudy et al. (2014) present a method that uses motion tracking to monitor activity around the user: the system can make the user aware of potential shoulder-surfers, or the system itself can hide certain information when required. Very little research has been done on using interface design to restrict shoulder-surfing. This is an area that needs attention as it is also potentially getting even easier with the growing trend for bigger digital displays in ATMs and other public terminals. With ATMs in particular, this trend reflects a fundamental change in financial services provision. Banks are keen to guide their customers to use ATMs, as opposed to traditional teller services. An industry survey of the future views of leading financial institutions and ATM operators found that 71% said they were planning to add new transactions to their ATMs e.g. enabling their customers to use an ATM for a video conference with financial experts in other locations. Most also intended to provide more customised services and targeted marketing via their ATMs. The survey also highlighted the need for these multi-functional ATMs to be flexible e.g. they may be used for video conferencing for some of the time but switched to only dispensing cash during the rush hour. (ATMmarketplace, 2014)

This type of new functionality and content places demands on the design of ATMs. Some of these features such as video conferencing and marketing, may benefit from a bigger display but this must not compromise users' privacy. The privacy of these larger displays can easily be improved e.g. by adding a privacy filter to restrict the viewing angle so that only the person standing directly in front can see the content, but very little is known about the user's perception of privacy. For example, a bigger display may feel less private, regardless of any technical privacy features. It may be possible to mitigate this and to support users' perception of privacy by careful design of the user interface.

This research aims to understand the tension between banks' preference for larger displays and users' desire to keep information private. It is hypothesised that careful design of the user interface could alleviate users' privacy concerns and perhaps increase the perceived privacy of the transactions. The initial exploratory stage of the study, reported in this paper, focussed on identifying which areas of the display felt private and which felt less private. These could then be mapped onto corresponding areas of the display, allowing different types of content to be presented and prioritised appropriately

2. Method

In this exploratory stage of the project, groups of 2 – 3 people were invited to take part in a user research session (n=51; 23 women and 28 men).

The equipment used in the study comprised of:

a) a non-functional model of the new ATM range: This range offers the option of a large touchscreen (19", 305 x 380 mm), a traditional physical keypad, and a touchscreen PIN pad. The physical keypad is positioned to the right of the screen as opposed to below the screen, as is common. It was important that both on-screen and physical PIN pads were discussed during the research sessions, as we wanted to explore participants' preferences on the PIN pad locations.

b) a paper prototype simulating the screens: Each screen required for a banking transaction was printed on a sheet of paper the same size as a 19" touchscreen. Some of the interface elements on those screens such as the on-screen PIN pad, were printed on separate pieces of paper so that they could easily be moved around and arranged in different layouts using Blu-Tack.

In a role-play scenario, one participant in each group was assigned the ATM user role and instructed to use an ATM prototype to first check their balance and then withdraw some cash. The other participant(s) were asked to play the role of a shoulder-surfer. (Figure 1) Participants were encouraged to discuss their experience of privacy and instructed to place the moveable interface elements where they felt they would be most private. (Figure 2) Participants were also asked to outline the most private area of each screen with a green marker and the least private area with a red marker. (Figure 3) The shoulder-surfer's point of view was discussed but no detailed data was collected about what they could and could not see.

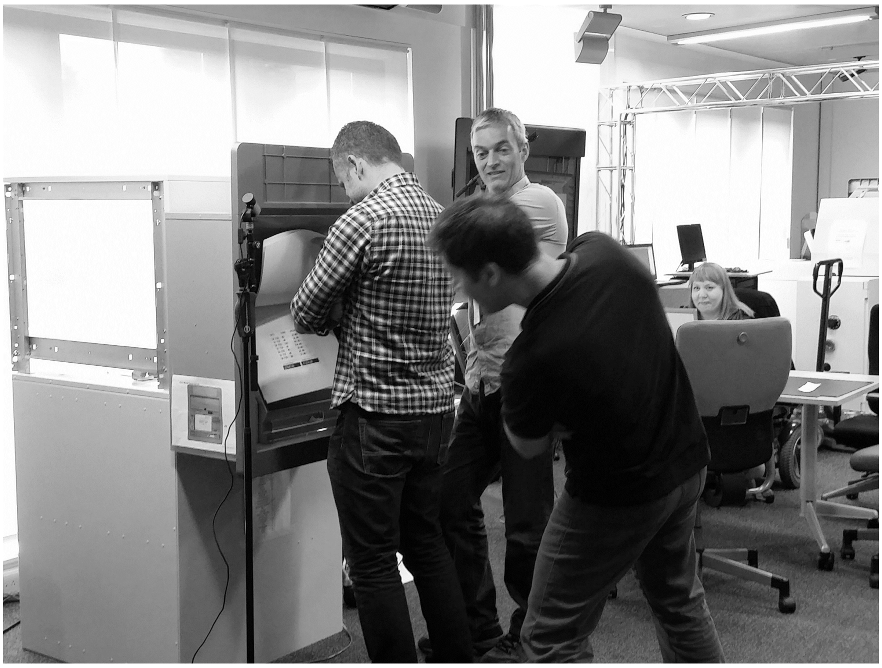

Figure 1. Role-play with one participant acting as the ATM user and another as a shoulder-surfer. The researcher is flipping the screens of the paper prototype.

3. Results

The data consisted of the sheets of the paper prototype, each with the red and green sketches denoting the private and non-private areas. To analyse the sketches, each sheet was divided into a grid of 3x3 cells using a transparent overlay that was placed over the sketch (Figure 4). A numerical value was given to each of the 9 cells according to the colour of the markings in it: a negative value for red (non-private) cells and a positive value for green (private) cells. Table 1 illustrates this process. The numerical values allowed: aggregation of the sketches across all participants; and calculation of the perceived privacy of each screen area

Table 1. Analysis of each cell converting red and green markings to numerical values

Sketch in the cell	**Researchers' interpretation**	**Numerical value**
Primarily red	Cell considered non-private	-2
Some red	Cell considered somewhat non-private	-1
Neither red nor green	Cell considered neither non-private nor private	0
Some green	Cell considered somewhat private	+1
Primarily green	Cell considered private	+2

Figure 5 shows the total sum in each of the 9 cells across all participants.

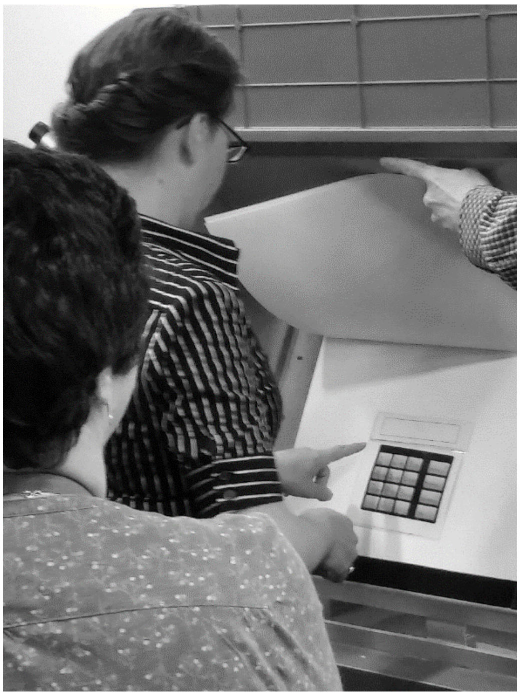

Figure 2. A paper prototype was used to simulate the screens of a basic ATM transaction. Participants could move the interface elements.

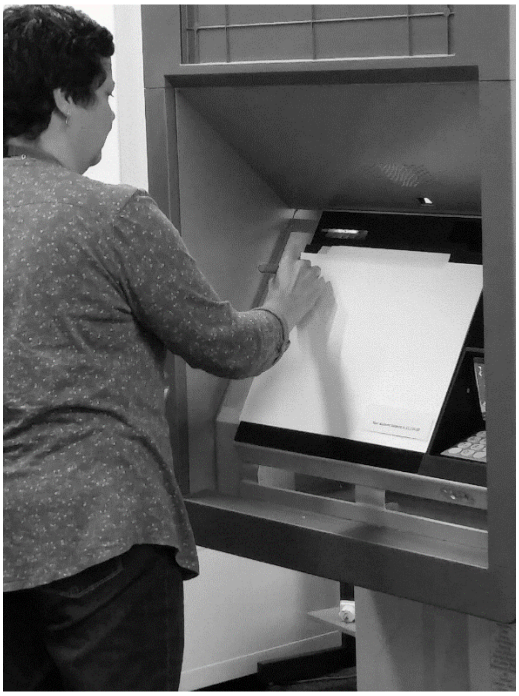

Figure 3. Participants were asked to sketch on each screen those areas which felt most private (in green marker) and those that felt least private (in red marker).

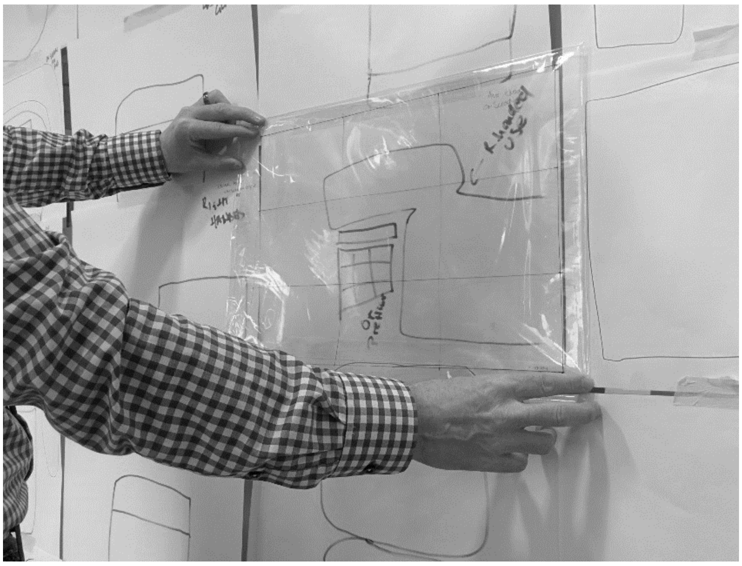

Figure 1. Each sketched screen was overlaid with a transparent 3x3 grid to give a numerical value to each cell in terms of its perceived privacy

305 mm

-69	**-41**	**-52**
-44	**+111**	**-7**
-31	**+127**	**+49**

380 mm

Figure 2. A 19" touchscreen (physical size 305 x 380 mm) divided into a 3x3 grid, and the privacy ratings for each of the 9 cells. Negative values mean non-private areas and positive values mean private areas.

Based on these ratings, the centre, lower centre and lower right were felt to be the most private areas of the screen. The least private areas were towards the top and top left. The positive and negative ratings were also visualised in the form of heat maps displaying the entire ATM interface including the physical interaction points (the card reader and the keypad) to the right of the display. These results show that there is a clear preference for the centre, lower centre and lower right areas of the screen for private information (Figure 6). Correspondingly, the area that is perceived to be the least private is the top of the screen and the top left corner (Figure 7).

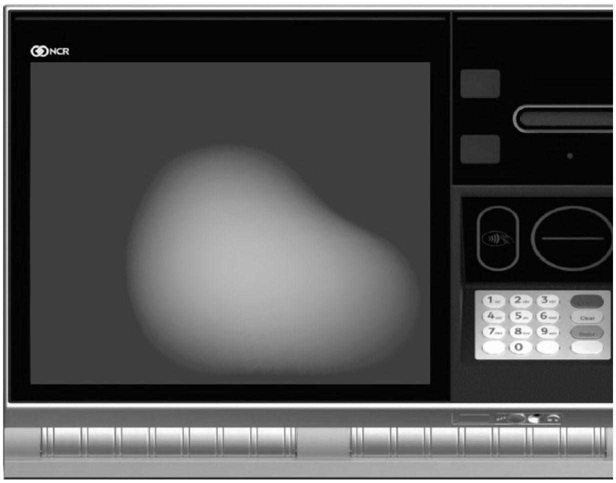

Figure 3. The areas of the screen that the participants marked as most private

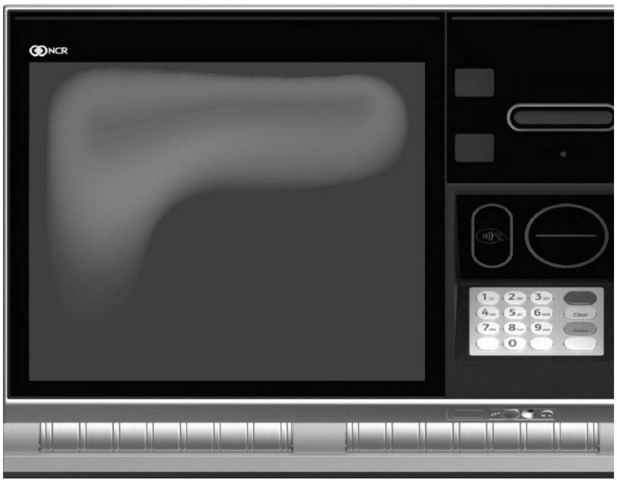

Figure 4. The areas of the screen that the participants marked as least private

It is interesting to note that the areas felt to be the most private are near the physical interaction points on the right. It may be that participants were inclined to shield the card reader and keypad area with their body, and so preferred to have the on-screen interaction near. Limiting the interaction points to a smaller area may then enhance users' perception of privacy because they are better able to shield the interaction with their bodies.

Although the centre of the display was thought to be the most private area, the lower right corner was rated very private as well. So there might be value in positioning the on-screen PIN pad in this area. The user can be guided towards the appropriate action by placing interaction points that are related to each other in close proximity such as the card reader and the PIN pad (whether on-screen or physical). The tight spatial relationship could be used to enforce the semantic relationship between these interface elements. Positioning the on-screen PIN pad near the physical keypad could also makes interaction more consistent for users between ATMs with an on-screen PIN pad and those with a physical one.

There are some usability challenges with the on-screen PIN entry: it is positioned higher and is less reclined compared to the physical keypad. This may have an impact on its perceived privacy and comfort of use. Further research is required to understand how users would interact with an on-screen PIN pad. The benefits of an on-screen PIN pad are that it can be moved and resized, but these features could not be tested properly with a paper prototype.

4. Discussion and Conclusion

Although the trend towards larger ATM screens is primarily driven by banks, large displays do have many advantages for users as well. They can be used to: provide richer visual experiences, including subtle animated transitions, to direct the user's attention and guide their behaviour; and to offer more on-screen space that can be used to deliver additional functionality, information or instructions. Larger touchscreens can also help improve the accessibility of ATMs e.g. by providing higher contrast and magnification capability for partially sighted users, and larger buttons and other interaction points for people with reduced dexterity, tremor or reduced hand-eye coordination.

There is however a potential conflict between big bright displays and the privacy, both perceived and actual, of sensitive information. This paper reports the early stages of a research project to explore the perceived privacy of on-screen information in the context of financial transactions at an ATM. We used a role-play method combined with paper prototyping to elicit discussion about the perceived privacy from the perspectives of both an ATM user and a potential criminal shoulder-surfing to obtain sensitive information.

The results of this exploratory work indicate that large screens do provide adequate privacy if the positioning of user interface elements is carefully considered. The data reveal that participants had clear preferences for the most and least private areas of the 19" screen. The centre, lower centre and lower right areas were considered to be the most private, while the top of the screen, particularly the top left corner was perceived to be the least private.

These results have already informed the design of the user interface for the new ATM range. An interaction zone (outlined in white dashed line in Figure 8) places the software interaction points in proximity with the hardware interaction points. The benefits of this interaction zone are two-fold: 1) it puts these elements in an area of the screen that offers best perceived privacy; and 2) it minimises the amount of user movement required and allows users to physically shield the interface.

This early exploratory work highlights the complexity of perceived privacy and the need to investigate it in more detail. Further research on perceived privacy is already underway to: explore the effects of e.g. screen size and the type of content shown on the screen; consider users' personal characteristics and preferences, such as handedness; and learn how technical features such as a screen filter or on-screen camera feed to show the user's surroundings, could help.

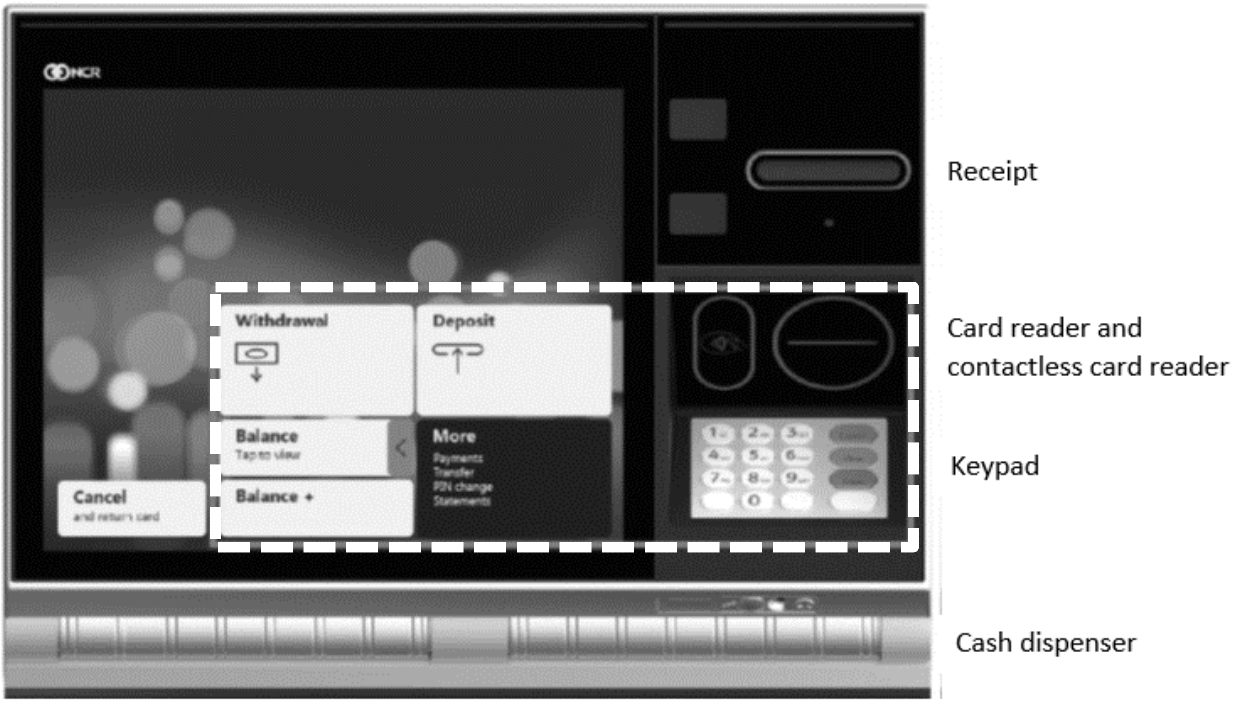

Figure 5. The ATM user interface consisting of the physical user interface with its hardware modules and the graphical user interface designed according to the privacy preferences identified in this study. The interaction zone is outlined in white dashed line.

Acknowledgements

The authors are indebted to Mike McKenna whose work was instrumental in facilitating the research sessions, analysing the data, and creating the visualisations and heat maps.

References

ATMmarketplace (2014) 2014 ATM Software Trends & Analysis. Networld Media Group.

Brudy, F., Ledo, D., Greenberg, S. & Butz, A. (2014) Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays through Awareness and Protection. Research Report 2014-1056-07, Department of Computer Science, University of Calgary, Calgary, Alberta, Canada.

De Luca, A., Langheinrich, M. & Hussman, H. (2010) Towards Understanding ATM Security – A Field Study of Real World ATM Use. In L.F. Cranor (Ed) Proceedings of the Sixth Symposium on Usable Privacy and Security [Article 16]. New York, NY: ACM.

Honan, Brian (2012) Visual Data Security White Paper. Secure – European Association for Visual Data Security. Retrieved on 7 October 2016 from <http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf>

Little, L. (2003) Attitudes towards technology use in public zones: the influence of external factors on ATM use. In CHI '03 extended abstracts on Human factors in computing systems [pp. 990 – 991]. New York, NY: ACM.

Mahansaria, D. (2009) Secure Password Entry Scheme in ATM Network which is Resistant to Peeping Attacks. International Journal of Engineering and Technology Vol.1, 2, 1793 – 8236.

Roth, V., Richter, K. & Freidinger, R. (2004) A PIN-entry method resilient against shoulder surfing. In B. Pfitzmann & P. Liu (Eds.) Proceedings of the 11th ACM Conference on Computer and Communications Security [pp.236 – 245]. New York, NY: ACM.

Shorter Oxford English Dictionary (2007). 6th edition. Oxford University Press, 2007.

Tari, F., Ant Ozok, A. & Holden, S.H. (2006) A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords. In L.F. Cranor (Ed) Proceedings of the Second Symposium on Usable Privacy and Security [pp.56 – 66]. New York, NY: ACM.